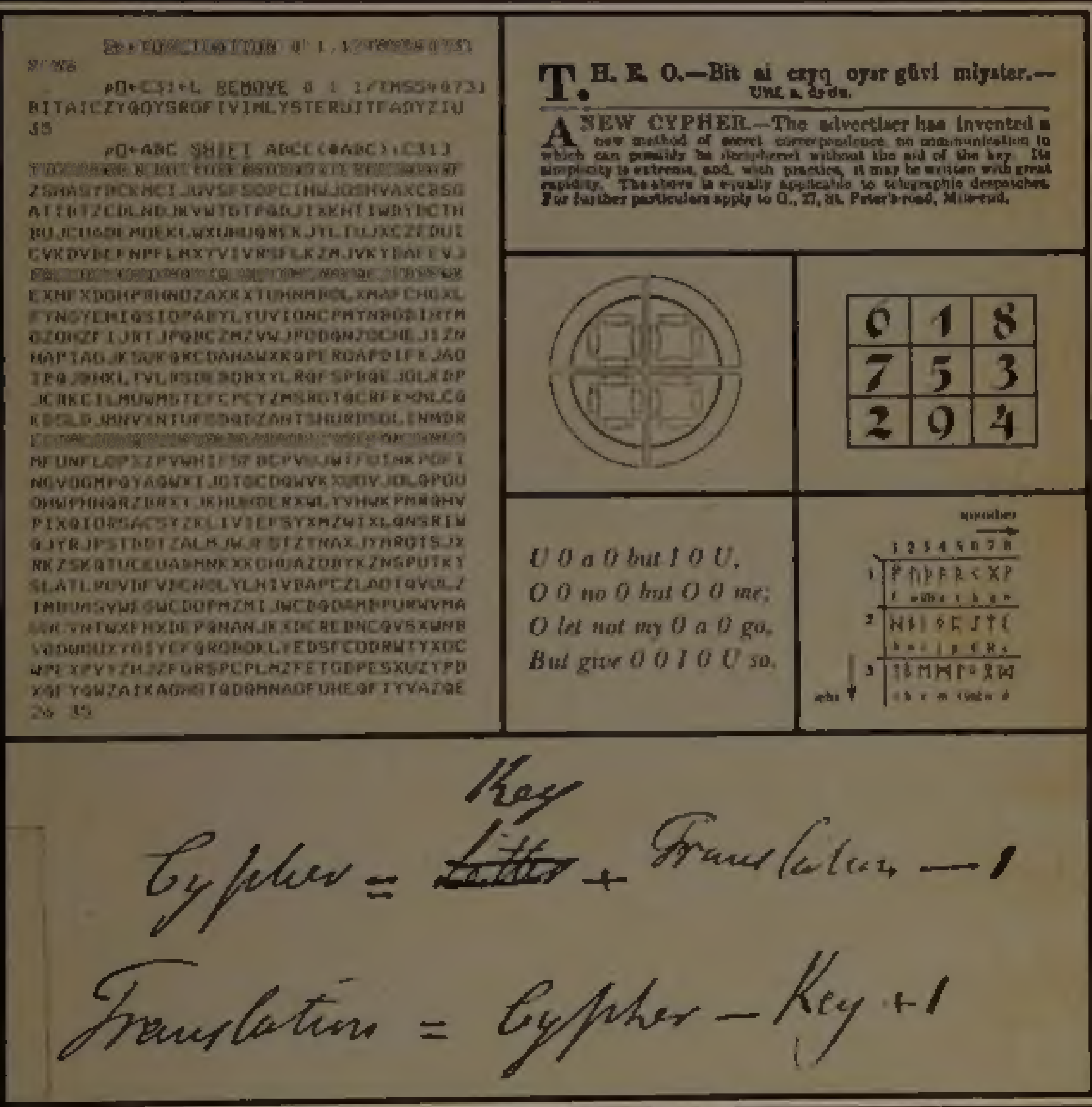
Ole Immanuel Franksen

Mr. Babbage's Secret

The Tale of a Cypher – and APL



MR. BABBAGE'S SECRET

Cover Illustrations

Front
APL solution of an advertisement in the Times, 31 July 1854.
The latter advertisement and another from the Times, 28 Jan. 1856.
The Viking fortress, Nonnebakken. *Courtesy Nationalmuseet, Copenhagen.*
A magic square.
Cipher poem to a young lady, by William Whewell.
The runic checkerboard alphabet, Futhark.
Babbage's formulation of his law for the Vigenère cipher. By permission of the British Library.

Back
Vigenère tableau from I. B. Lindenfels: Den hemmelige Skrivekonst
Kjøbenhavn 1819. The keyword in the second left column is:
"Danmark blomstre", *or Denmark blooming.*

Ole Immanuel Franksen

MR. BABBAGE'S SECRET

THE TALE OF A CYPHER

– AND APL

Foreword by

H. H. GOLDSTINE

Prentice-Hall, Inc.
Englewood Cliffs, New Jersey 07632

This edition published 1985 by Prentice-Hall, Inc., Englewood Cliffs, New Jersey 07632.

Funded by IBM

ISBN: 0-13-604729-7

Library of Congress Catalog Card Number: 85-60146

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

ISBN 0-13-604729-7 01

Prentice-Hall International, Inc., *London*
Prentice-Hall of Australia Pty. Limited, *Sydney*
Editora Prentice-Hall do Brasil, Ltda., *Rio de Janeiro*
Prentice-Hall Canada Inc., *Toronto*
Prentice-Hall Hispanoamericana, S.A., *Mexico*
Prentice-Hall of India Private Limited, *New Delhi*
Prentice-Hall of Japan, Inc., *Tokyo*
Prentice-Hall of Southeast Asia Pte. Ltd., *Singapore*
Whitehall Books Limited, *Wellington, New Zealand*

Foreword

In the fall of 1960, during my term as director of mathematical sciences at the Thomas J. Watson Research Center of IBM, Ole Immanuel Franksen joined my scientific staff as a NATO Fellow on leave of absence from the Electric Power Engineering Department of the Technical University of Denmark. This was in a period of very exciting explorations into new fields of computer applications, and I found in Dr. Franksen one of those young engineering scientists who helped to pioneer these explorations with vision and ideas. He stayed with us through 1961 and in that period I developed a close professional and personal relationship with him, which over the years has given me the opportunity of following his development of a unique systems approach to the general uses of computers.

Trained as an electric power engineer Franksen's original interest was in the design of electric machinery and power apparatus. His mentor, the late Professor L. Hyldgaard-Jensen, who later came to serve on the board of IBM Denmark, once gave me an account of Franksen's early computer work.

As the topic for his Master's Thesis in 1956 Professor Hyldgaard had assigned him the problem of clarifying the causes of unexpected heating problems in electric power generators under certain load conditions. Franksen succeeded in boiling the question down to an electromagnetic field problem, but he could not verify his model without unsurmountable numerical calculations. By accident Professor Hyldgaard had happened to be in a meeting in which representatives of IBM Denmark also participated. Although no digital computer, as we understand the term now, existed in Denmark at that time Professor Hyldgaard felt sufficiently encouraged by their account of IBM's punch card equipment to ask the company for assistance. Engineering design problems were at that time considered far outside the field of application of such equipment, but it was soon agreed that the possibilities needed to be investigated. Franksen was therefore given access to a wire-programmed IBM 602A Punch Card Calculator and, recasting his problem into matrix form, he eventually obtained numerical results explaining the anomalous temperature measurements.

Today when CAD or computer aided design is almost a catch-word, this may seem commonplace. But in 1956 when only very few even thought of the possibility, such applications opened up an entirely new future. In any case, Professor Hyldgaard was enthusiastic, and he had Franksen employed as an assistant professor in order that he could carry through a doctoral project investigating this new tool. In connection with the ASEA company in Sweden it was decided to let Franksen try to attach the problem of computerizing some of the many calculations involved in power transformer design, using the Danish computer DASK which was completed in 1958.

To learn the trade in an industrial environment Franksen spend part of the time in the ASEA transformer plant in Ludvika, Sweden. Since he had no access to a computer during 1957, he decided to organize and document the collected experiences of the expert transformer

designers by means of flow charts at the same time that he checked this information (by hand calculation following the flow charts) against an extensive file of detailed technical descriptions of previously manufactured transformers. In this way he discovered what no one around him had thought possible that it would indeed be feasible to have the computer take over the entire design process, replacing human brain power by a cut-and-try computer search technique for an optimal transformer satisfying the customer's specification. Implemented on DASK in a program package of 12 to 15,000 instructions in hexadecimal machine code he proved his point, thus launching the Scandinavian electric power industry into a new era. In 1959, after having received the Ph.D. degree for this work, Franksen won a NATO Fellowship for two years and went to the United States for further studies.

Another catchword of today besides CAD is CAM, computer aided manufacturing: a concept often identified quite narrowly with special-purpose software for the 2- or 3-dimensional representation of geometrical objects on a computer screen. However, we should not forget that software for interrelating design with production and for planning and controlling production is of essential importance in this connection. During his work on the transformer project Franksen had perceived early on that, with the advent of the computer, the artificial barrier between design and production would gradually disappear. Through the good offices of the late Philip L. Alger, the well known induction motor designer who originally had brought Gabriel Kron to General Electric, he was invited by that company to participate in, perhaps at the time, one of the most ambitious industrial projects in this direction. This was the Automated Requisition Engineering Project, called AREP, in GE's medium ac motor department in Schenectady, New York. Here, motor design, production preparation, drawings, administrative systems and economic reporting were integrated by means of the computer; and to deal with the vast amount of data new concepts were developed which only much later were formalized and given names as part of computer science.

It was also during his stay in Schenectady that Franksen became friends with Gabriel Kron whose revolutionary theoretical approach would come to have such a profound influence on his later scientific contribution. As Franksen saw it, the computer had wrought a revolution in engineering industrial practice which necessitated a fundamental revision of its theoretical foundation in order to permit these novel advances to become teachable parts of a scientific discipline. After having visited some sixteen universities on the East coast of the United States and interviewed the foremost proponents of electrical engineering education there, he discerned that essentially there were two schools confronting each other: energy conversion and the electrical network approach. His discussions with Kron soon convinced him that already many years earlier Kron had brought these two opposed views together in a unified theory. Furthermore, that Kron's tensorial approach in terms of multidimensional, rectangular data arrays was the novel kind of formulation that was needed to match the future capabilities of the computer. Kron was a genius and, to those who met him like Franksen, a fireball of inspiration; but his exposition was marred by severe shortcomings which even today cause discus-

sion. Therefore, to reach a deeper understanding Franksen turned to the inner circle of scientists who had worked with Kron for years. Chief among them was a collaborator of Einstein's, the brilliant tensor specialist Banesh Hoffmann, with whom he became fast friends.

Another problem area which much occupied Franksen, was the identification and formalization of the heuristic design process and the associated discrete optimization. At IBM several research projects were under way in this direction like Arthur L. Samuel's computerization of the game of checkers and Ralph Gomory's work in integer programming. Naturally while at IBM Franksen took advantage of this situation, and at the same time he made it his business to meet and discuss with IBM scientists and engineers who, like J. P. Roth and F. H. Branin, Jr., had taken an active interest in Kron's ideas. The latter in particular much influenced Franksen's view on how to integrate Kron's network theory with the uses of computers; and it was through these discussions that he became convinced that it would be possible to develop macroprogramming languages which would enable the end user interactively to perform computational experiments in terms of Kron's rectangular arrays, much the same way as the engineer used "to hook up" models on an analogue computer.

Returning to his native Denmark he was initially charged with the development and teaching of a new course in computerized design of electric machinery. Simultaneously he started publishing his ideas on the formulation of an interdisciplinary systems approach, integrating Kron's theory with the uses of macroprogramming languages. In 1964 he was promoted associate professor with the responsibility of developing a new engineering discipline known as systems science.

Surrounded by a group of enthusiastic graduate and doctoral students Franksen soon had research on systems science and computer applications taking flight by means of joint projects with Danish industry as well as with universities in England and abroad. Already in 1965 he was awarded the LK-prize of Da.kr. 25,000-- for his scientific contributions, being the first recipient of this distinguished honour of Danish electric power industry. The same year the Ford Foundation granted his university an IBM 1800 computer to be placed under his direct supervision. This was indeed a rare international recognition because this computer was given, as the Ford Foundation wrote in its annual report, in an "effort to strengthen American Education in engineering design". As part of the conditions of the grant Franksen therefore spent the following summers giving short courses and lectures at different American Universities, ending up as a visiting professor at UCLA in 1969. During the latter stay he also participated in a statewide lecture series of the University of California.

In his endeavour to arrive at a truly unified systems approach Franksen studied not only the engineering and physical disciplines but also economics, carefully reading the original contributions of the great masters of the past, whether in English, German, French, or one of the Scandinavian languages. In this way he succeeded in explaining fundamental models like the Walrasian of economics by physical analogies at the same time that he was able to present some intriguing discoveries. For example, that Fourier had lectured on linear pro-

gramming to the Paris Academy in 1824, and that by 1838 two of his "students", Cournot and Ostrogradsky, had given a tentative formulation of what is today known as the 1950 Kuhn-Tucker theorem on non-linear programming. In fact, clothed in its classical mechanics form the original formulation of this theorem may even be found in the Handbuch der Physik *at the turn of this century.*

These historical studies gave Franksen a unique background for presenting a novel view on systems science, rooting Kron's ideas in the main stream of the traditions of science. Together with his Norwegian colleague Professor Øyvind Bjørke of the Production Engineering Laboratory at the University of Trondheim, he began to promote a distinct Scandinavian systems approach, having published the proceedings of two so called Lerchendal conferences in 1978 and 1981 with a third to appear in 1984. Also Franksen's scientific reputation was recognized in Sweden. Thus in 1973 he was the opponent ex officio of the Faculty of Social Sciences at Gothenburg University at a doctoral degree in economics, while in 1978 he served in the same capacity for the electrical engineering faculty at the Royal Institute of Technology in Stockholm at a doctoral degree in engineering. The latter faculty also appointed him in 1974 to serve on the valuation committee for a new chair in electric power conversion.

At the time that Franksen undertook this fundamental work, he never lost sight of the ultimate criterion of industrial usefulness. Over the years he has had his graduate and doctoral students work in joint research projects on computer applications not only with industry, but also with banks, insurance companies, and governmental institutions. The success of this approach may perhaps be judged by the fact that almost half of the funding for his doctoral candidates has come from these private sources. Indeed, it was for this contribution to fundamental as well as to applied systems science that in 1982 he was awarded an honorary gift of Da.kr. 70,000-- by the Ellen and Hans Hermer Foundation, which is under the permanent trusteeship of the rectors of Copenhagen University, the Technical University of Denmark, and the Royal Veterinary and Agricultural University.

*Franksen's historical interest in the life and work of Charles Babbage can be dated back to 1965 at which time IBM, as a result of the endeavours of my late friend Viggo Troels-Smith, the managing director of IBM Denmark, granted the Technical University an IBM 7090 installation. To celebrate the inauguration of the new computing center NEUCC (the Northern Europe Computing Center) Franksen was asked to write a popular book, describing the evolution of computers from the abacus to the digital computer. In the preparation for this book he found Babbage so fascinating a subject, that since then he sustained this interest by source studies in the British Library and elsewhere. Thus in 1981 he published a paper: "Mr. Babbage, the Difference Engine, and the Problem of Notation" (*Int. J. Engn. Sci.*), in which by simulation in the well known programming language APL he traced the origin of recursiveness and programmed conditionals.*

About 1972, having discovered the public debate between Thwaites and Babbage in the 1854 volume of the Journal of the Society of Arts, *he succeeded in recovering the*

message in Babbage's enciphered challenge. During a subsequent visit in the British Library he procured a set of rather poor photocopies of Babbage's manuscript on ciphers and deciphering. In his spare time over the years since then he has tried to get some meaning out of these unpublished notes, guessing the approach Babbage might have taken, implementing it in APL, and painstakingly trying to compare his results with Babbage's in order to discover the special cases which might explain how Babbage actually went about it.

In his other historical studies he had accidentally come across other great scientists who had cultivated an interest in cryptography, and he started to recognize a common pattern which reminded him of his early computer work. It struck him that these great men were primarily problem-solvers with uncanny intuitions, and that deciphering in some way or other had been a training ground for sharpening their insights, their senses of abstract pattern, and their innovative powers in their attempts to cast real life problems into computable mathematical forms. This discovery intrigued him, and he started developing a cryptographic tool-kit in APL, which he tested by cracking enciphered advertisements from the "agony columns" of Victorian newspapers.

This hobby gave him the idea that here was a fascinating field of application which, amenable to a rich and inspiring variety of mathematical techniques, would be well-suited for introducing APL to the young at the gymnasium level or even earlier. At this introductory level of computer education one needs to overcome the feeling that applied problems require specialized knowledge. The beauty of this subject is that the young student needs little or no formal mathematical background to start to work.

In 1981, having been invited to Helsinki by the Finnish Academy of Technical Sciences to give a lecture, he also met informally with his colleagues of FinnAPL, the Finish APL Association. Here, the discussion happened to touch upon the problem of high school computer education and APL; as someone lamented that all possible problems at this level were drab, Franksen remarked that this was because they did not follow Babbage in his approach to secret writing. Knowing Franksen's historical interest in Babbage, he was soon lured into a description of his hobby and his uses of APL; and from this incident followed a formal invitation from FinnAPL asking Franksen to write the present book which will be published in connection with the APL84 Conference in Helsinki in June 1984. IBM in the Scandinavian countries was approached for funds, and Mr. Johan Teglhøj of IBM Denmark played a vital role in carrying the application to a successful result.

John von Neumann, my late friend and colleague of the pioneering days of the ENIAC, EDVAC and IAS computers, considered it a fundamental thesis that, even if the mathematical criteria of success are almost entirely aesthetical, the ideas of mathematics originate in experience. This explains, as he saw it, the quite peculiar relationship that mathematics has to any science which interprets experience on a higher than purely factual level. Mathematics provides the penetration and capacity to see the general in the particular and the particular in the general, enabling these sciences to produce elegant as well as useful results.

This thesis is reflected in the present book. Although it may be read as an entertaining account of the cryptographical works of Babbage and others, the reader will find that the subject area of 19th century secret writing is not a goal in itself, but rather a vehicle. Neither is it a textbook presenting an educational introduction to APL. What fascinated Franksen and, I think, what will fascinate the reader, is Babbage's groping towards an understanding of the innermost nature of data and data operations.

Throughout the history of science there runs a theme that geometry is the mother of mathematical invention, whereas analysis and algebra are the necessary implements for statements of any complexity. From Franksen's early work on macroprogramming languages and his uses of APL since 1969 the imprint of this theme has been his gradual clarification of the notion of data as geometrical objects. It is in this light that he sees Babbage's attempts to cast cryptography into a formalized mathematical formulation. His illustrations in APL of Babbage's work provide explanation of and meaningful context for this geometrical view on data. Indeed it is the formulation of the cryptographical problems in APL which most convincingly puts an end to the mental straitjacket originating in the constraints of the early computers that data must be dealt with at the scalar level of a single number or a single character. It is his intriguing thought, given a popular exposition in this book, that the data concept of APL reduces to the definition of a geometry in the sense of Felix Klein's famous Erlanger Program of 1872. This opens an entirely new perspective in the educational integration of the computer into the traditional sciences and their areas of application. Therefore I find it important that this book should reach a wide international audience of educators and professionals in the computing fields.

The Institute for Advanced Study, Princeton, NJ

Herman H. Goldstine

Herman H. Goldstine

Contents

Prologue

A tale, even if true, must have a beginning and an end. To put a date on the end we could say that it was December 8th, 1857. Prior to that date, in the correspondence between him and various people on the subject of ciphers, Charles Babbage made comments such as "*the paper on cyphers I intend to write ...*"[1]) However, in a letter written that day in response to a request on examining or solving a new cipher, Babbage informed the unknown addressee that he had been obliged to give up his "*proposed work on cypher*" for the time being. This letter, the draft of which has been transcribed in figure 1[2]),denoted the final end. As it turned out, his work on ciphers was never resumed.

Dating a beginning of our tale is obvious to any reader of Babbage's autobiographical *Passages from the Life of a Philosopher.*[3]) Published 1864 this book aimed at making "*less unpalatable*" the description of "*those Calculating Machines on which I have*

Sir,

The object of my proposed work on Cypher is not exactly what you suppose, but my time is now so entirely occupied that I have been obliged to give it up at least for the next two or three years.

However under any circumstances I should decline the challenge you propose on grounds which I have stated to the Sec^y of the Society of Arts in a letter printed about two years ago in the proceedings of that Society.

I send by this post a pamphlet in which I have marked page 14 of the preface.

If you should think it worth the trouble and should send me in cypher a portion of it as mentioned I will place it amongst my papers and should any friend apply for a difficult cypher I will put it into his hands.

In any case it is unnecessary to return the pamphlet.

I am Sir, Your Ob^t Ser^t

8 Dec^r 1857

Figure 1. Transcript of a letter from Charles Babbage to an unknown addressee. From a draft among his scientific papers in the British Library (BL, Add.Ms. 37205, F.198)[2])

PASSAGES

FROM

THE LIFE OF A PHILOSOPHER.

BY

CHARLES BABBAGE, ESQ., M.A.,

F.R.S., F.R.S.E., F.R.A.S., F. STAT. S., HON. M.R.I.A., M.C.P.S.,

COMMANDER OF THE ITALIAN ORDER OF ST. MAURICE AND ST. LAZARUS,

INST. IMP. (ACAD. MORAL.) PARIS CORR., ACAD. AMER. ART. ET SC. BOSTON, REG. OECON. BORUSS., PHYS. HIST. NAT. GENEV., ACAD. REG. MONAC., HAFN., MASSIL., ET DIVION., SOCIUS. ACAD. IMP. ET REG. PETROP., NEAP., BRUX., PATAV., GEORG. FLOREN, LYNCEI ROM., MUT., PHILOMATH. PARIS, SOC. CORR., ETC.

"I'm a philosopher. Confound them all—
Birds, beasts, and men; but no, not womankind."—*Don Juan*

"I now gave my mind to philosophy: the great object of my ambition was to make out a complete system of the universe, including and comprehending the origin, causes, consequences, and termination of all things. Instead of countenance, encouragement, and applause, which I should have received from every one who has the true dignity of an oyster at heart, I was exposed to calumny and misrepresentation. While engaged in my great work on the universe, some even went so far as to accuse me of infidelity;—such is the malignity of oysters."—"*Autobiography of an Oyster*" *deciphered by the aid of photography in the shell of a philosopher of that race,—recently scolloped.*

LONDON:

LONGMAN, GREEN, LONGMAN, ROBERTS, & GREEN.

1864.

Figure 2. Facsimile of the title page from *Passages from the Life of a Philosopher* published in 1864. The sham quotation was appreciated by Babbage's contemporaries as a witty reference to the dialogue where Plato let Socrates say: "If you had no power of calculation you would not be able to calculate on future pleasure, and your life would be the life, not of a man, but of an oyster or *pulmo marinus.*" *Philebus*, 21.

spent so large a portion of my life" (see figure 2). Devoting the better part of a chapter to a popular account on deciphering Babbage said by way of introduction:

> *"Decyphering is, in my opinion, one of the most fascinating of arts, and I fear I have wasted upon it more time than it deserves. I practised it in its simplest form when I was at school. The bigger boys made cyphers, but if I got hold of a few words, I usually found out the key. The consequence of this ingenuity was occasionally painful: the owners of the detected cyphers sometimes trashed me, though the fault really lay in their own stupidity."*

Born in South London on December 26, 1791, [4]) Babbage also died in that city on October 18, 1871. Since he went up to Cambridge University in 1810, the first decade of the nineteenth century would mark a beginning of our tale acceptable to most historians.

Yet to Babbage himself February-March, 1846, would be the decisive date. Because in this period, deciphering a challenge posed by his nephew Henry Hollier, he achieved the initial breakthrough, turning his life-long passion since the years of boyhood into a mathematical science.

Henry had applied a very general type of cipher, now known as a *Vigenère* after a 16th century French diplomat and scholar. Babbage's extraordinary feat was to give the law of this cipher an algebraic form, structurally akin to the conservation law of energy conceived within the same decade. Of course, Babbage had no idea of this mathematical analogy, but the fact remains that he was guided by similar intuitive ideas. As the notion of energy was introduced in physics to describe the indestructible forces of nature, changing only in form between mechanical work and heat, so Babbage considered the content of meaning as the indestructible element of information, changing only in form between plaintext and cryptogram. Indeed, as he stated in his *Passages:*

> *"There is a kind of maxim amongst the craft of decypherers (similar to one amongst the locksmiths), that every cypher can be decyphered.*
> *I am myself inclined to think that decyphering is an affair of time, ingenuity, and patience; and that very few cyphers are worth the trouble of unravelling them."*

Babbage's great achievement was to be the first to cast this intuitive maxim into the mathematical form of a *cryptographic conservation law.* Further, that he recognized as a man of science, the importance of this step and attempted to explore its consequences. His proposed work on cyphers did not belong to the several schemes, writing novels or building an automaton to play tic-tac-toe, which Babbage in these years told friends he was considering to help finance the construction of his Analytical Engine. It was not the popular account on ciphers and deciphering

expected by the unknown recipient, presumably a gentleman amateur, of his letter of December 8th, 1857 As stated in this letter: "*The object ... is not exactly what you suppose*". No, the object was a scientific treatise on the ramifications of the discovery of law.

It is the untold tale in his proposed work on this discovery which we shall attempt to unravel. Though no manuscript or fractions thereof have been discovered, if ever written at all, circumstantial evidence of various nature will help to unearth the scaffolding by means of which Babbage intended to erect this intellectual structure. Of course, even at this point there will be loose ends, conflicting testimonies, and large holes in our knowledge for posterity to repair. While true in the sense that all the established facts will be presented in our tale as such, the problem confronting us may be compared to that of the archeologist who, having excavated an empty viking shipyard, strives to imagine the ships launched there.

In his other writings Babbage quite often found it convenient to explain himself by means of numerical illustrations or computational experiments. By hand calculations he simulated the workings of his life's obsession: the Difference Engine [5]) and the Analytical Engine. As befits the great pioneer of the modern computer he was, so to speak, an algorithmic thinker, always emphasizing the procedure by which the results are obtained

His work on codebreaking does not differ in this respect. Mechanical aids like cipher discs or slides, as he tells us, were his foremost tools. Hence, it is only by adhering to this approach that we can hope to derive some meaning from his cursory notes. In a tale, however, we are not bound by time or place. Therefore, instead of these mechanical means we shall supply Babbage with an APL-terminal, letting him perform interactively on the computer what in the usual parlance is known as *terminal sessions*. Becoming a tale, this licence, if not revealing the whole truth, will at least be true to the spirit of his work and his discovery.

Thus, couched in APL illustrations, the tale to be told here will have its roots in Babbage's experiences as a schoolboy, its mathematical breakthrough in his discovery February-March, 1846, and its final end in the letter of December 8th, 1857

The Philosophy of Decyphering

1.1 A List of Works

The reputation Babbage acquired in his time as a cryptographer, was not due to any publications of his on this topic. In fact, when he published the chapter on deciphering in his autobiographical *Passages* from 1864, he was already acknowledged by his contemporaries for his expertise and experience in the field. It was recognized simultaneously, of course, that as a gentleman he merely cultivated an interest. He was not a professional, working for the government like his 17th century predecessor, the famous mathematician John Wallis. Indirectly, this is also the message brought out in his letter to the editor of the Journal of the Society of Arts in 1855. Reprinted in figure 3 this letter, stating his *credo* on the art, was his only other publication on cryptography known to his contemporaries.

Yet, to the inner circle, his private friends and acquaintances, it was well known that in 1854, writing anonymously under the pseudonym "C", Babbage published two more letters in this journal, successfully taking up a challenge by a Mr. Thwaites who happened to reinvent the Vigenère cipher. The importance of these two letters relative to Babbage's contribution to cryptography, is perhaps best illustrated by the fact that ten years later Babbage included them as items 66 and 67 in his list of printed papers appended to the *Passages*.[6])

The public dispute in the Journal of the Society of Arts between Thwaites and Babbage, is perhaps the most important source document to Babbage's proposed work on ciphers. The letter to the editor, published the following year in Babbage's own name, is Babbage's uncompromising closing of this debate. Although later, in his usual rush, Babbage forgot to include the latter letter in the list of printed papers in his autobiography

The results documented in the two anonymous letters are indeed astounding, but unfortunately Babbage did not disclose how he arrived at them. Apparently this was on purpose, for among his scientific papers in the British Library I found part of a draft of one of these letters that clearly enters upon an explanation which, however, is neither finished nor included in the printed version.[7]) Therefore, it would appear that Babbage decided to save the presentation of his approach for

the proposed work on ciphers, wisely reasoning that in a public debate scientific arguments usually carry little weight. It will thus appear that in our tale this public exchange of letters will come to play a central role, and so for the benefit of the reader it has been reproduced in this book from the old pages of the Journal of the Society of Arts.[8])

While these brief publications are of central interest to our story, it is equally evident that they appeared in print far too late in time to have any influence at all upon his reputation as a cryptographer. Definitely, the only publication which might have contributed to his reputation in this respect, was the remaining entry on ciphers (listed as item 50) in the bibliography of his printed papers in the *Passages*. Printed in Francis Baily's book from 1835 on the first Astronomer-Royal, John Flamsteed, this publication is a letter from 1721-22 of about 900 words which Babbage deciphered from a kind of shorthand. Since just the plaintext is given in this work, the curiosity of the readers, however, could have been stirred only by Baily's description.[9])

The problem facing Baily was to establish the accuracy of Flamsteed's observations from the Royal Observatory at Greenwich. Since in his writings Flamsteed had vaguely hinted at an error of division of his mural arc, it became necessary for Baily to turn to other source documents in order to determine exactly the error of this astronomical instrument. Searching the original manuscript letters of Mr. A. Sharp, Flamsteed's assistant who divided the instrument, he was fortunate enough to find a letter, dated Jan. 27, 1721-22, from a Mr. Crosthwait, in which the latter questioned Mr. Sharp as to his knowledge of the existence of such an error. Baily continued the explanation in his book:

> *"The answer of Mr. Sharp is, agreeable to his invariable custom, written in short hand at the back of the letter: and my object was now to get this answer (if possible) deciphered. I applied to several gentlemen conversant with the art of stenography, but without effect; since the characters used by Mr. Sharp were not such as are explained in any of the books of the present day. On accidentally mentioning the subject to Charles Babbage, Esq. (Lucasian Professor of Mathematics at Cambridge) he very kindly offered to make the attempt; and I am happy to say with complete success. For, by a laborious and minute examination and comparison of all the parts, he at length obtained the key to the alphabet; and has thus enabled us to know Mr. Sharp's opinion on this interesting subject."*

To complete the story, the deciphered letter led Baily to the discovery that the errors arose from the table of refraction used by Flamsteed, leaving no reason to believe that the arc was erroneously divided.

An active astronomer himself Francis Baily lent his name to a phenomenon

CYPHER WRITING

Sir, – Doubtless the Council of the Society of Arts, as well as many other persons, who, like myself, have indulged in the fascinating art of deciphering, are continually called upon to occupy a very serious portion of their time, at the request of friends and even strangers, themselves unacquainted with that art.

Although I invariably decline such proposals, it may be of use to all parties to offer a few remarks on the subject.

To contrive a cypher which cannot be decyphered is not a question of any importance. To be really useful, the cypher must be capable of being easily and quickly written by the person using it, and as easily and quickly read by the person to whom it is addressed.

The art of decyphering resembles that of picking locks. The greater number of locks can be picked, and the only question is, what time each requires.

Mr. Hobbs, during the Exhibition of 1851, picked Bramah's challenge lock in about 56 hours.

The performers in the celebrated robbery of a bank in Scotland, spent three months in passing through three locks.

The last inscrutable cypher I decyphered, cost me thirty hours. Some have cost me four or five working days. A cypher, decyphered in Paris, for the French Government, occupied its decypherer fully during several months.

Any intelligent schoolboy can make a cypher which shall cost hours, and even days, for its solution, and it is a fact, that very clever men, who have not studied decyphering, have frequently invented cyphers which nothing (but their solution) could convince them were not inscrutable.

Under these circumstances decypherers have an understanding amongst themselves never to examine any challenge cypher unless the proposer has already proved his knowledge of the subject by having decyphered cyphers of admitted difficulty.

I am, yours faithfully,
CHARLES BABBAGE

Dorset-street, Manchester-square, Nov. 25th, 1855

Figure 3. Babbage's letter to the editor, *Journal of the Society of Arts*, No. 159, Vol. IV, Dec. 7, 1855, 40-41(Reprinted, Courtesy the Royal Society of Arts)

---

known as *Baily's beads*. The bright spots of sunlight which briefly appears around the edge of the moon's disk immediately before and after the central phase in a solar eclipse. In an article from 1834 the need for Babbage's Difference Engine is illustrated by the remark[10]): "*Mr. Baily states that he himself has detected in the solar and lunar tables, from which our Nautical Almanac was for a long period computed, more than five hundred errors.*" In this connection it may be of interest to record that Baily was a staunch advocate of Babbage's project on this computer. Thus, in a report of May 12, 1829, to the Royal Society of London in support of Babbage's claims as to the financial state of this project we find among "*the undersigned personal friends of Mr. Babbage*", as the report designate its authors, not only the name of Baily, but also

those of the Duke of Somerset and Dr. Wm. Henry Fitton.[11]) Although Baily shall take his leave here, both of the latter names will appear later in our tale.

Baily's account of Flamsteed's life makes fascinating reading even today, but I very much doubt that it contributed significantly to Babbage's image as a cryptographer. Rather, it would appear that it was through private discussions, perhaps entertaining guests at his famous soirées, that the knowledge spread of his ability in this field

1.2 Expert Witness

The year 1854 marks the culmination of Babbage's career as a cryptographer. In the autumn he took up the gauntlet of Mr. Thwaites in the pages of the Journal of the Society of Arts. Prior to that, in mid-July, it would appear that he testified in court as an expert witness, expounding how, at the request of the lawyers, he had solved some enciphered correspondence. As it turned out this correspondence happened to decide the case. A fact, which may well explain Babbage's reluctance to use his own name in the public debate with Mr. Thwaites.

The salient points of this law suit: communications from the lawyers and from the father of the one party to Babbage, and the crucial fragment of evidence translated by the latter, are transcribed in figures 4A-G (see pp. 21-23) from the documentation I found among Babbage's papers in the British Library.[12]) Although deplorably incomplete, these few pieces of information form a story of their own. An account of passion and tragedy, but also a rare glimpse of Babbage's working mode when solving a cipher.

To place this documentation in perspective I may offer some additional facts, derived from other of Babbage's papers in this collection.

The earliest date on one of the worksheets, giving evidence of his attack on the cipher, is 20 June 1854.[13]) We may assume, therefore, that, in the intervening period since the early exchange of letters in April, the barrister, Mr. A. W. Kinglake, had tried in vain to crack the cipher. Apparently its solution also caused Babbage some trouble. For in a letter, dated July 15, 1854, Kinglake acknowledges the receipt of Babbage's initial solution by the words: [14]) *"I am indeed greatly obliged to you. If I had foreseen the amount of trouble which I should be assuming to you, I think I should never have ventured to ask such a favour of you"*. He goes on to say that he will instantly communicate *"the contents of your first letter"* (i.e., the first of the enciphered letters) to the solicitor, Mr. John S. Gregory, whom he describes as *"as a very gentlemanlike old man, & a member of the Athenæum"*, the distinguished literary club of London.

Already the same day, Gregory communicates directly to Babbage for the first time[15]): *"My kind friend Mr. Kinglake has sent me your note of this days date ..."*, asking

Lincoln's Inn, April 20, 1854

Dear Sir,

I recollect that once when I had the pleasure of meeting you – now long ago – you interested me very much by some information which you gave me on the subject of deciphering conventional signs.

I am Council in a case which has some curious features in it, as there are a quantity of writings in cipher which it is deemed important to have interpreted. The Solicitor who instructs me is at a loss to find a person capable of doing this, and it has occurred to me that you might possibly know of some one who has given his attention to this subject, and who (in a professional way) would undertake the duty of deciphering the writings in question. If you should know such a person I should be glad to recommend him to the Solicitor who instructs me

I believe that the cipher in question is a simple one, & that the "key" is partly known, but the writings are voluminous, & therefore the mechanical labour of translating them would be considerable, & [erasure] *the fitte t person for the labour would be some young man of energy who can command leisure hours*

I must trust to your kindness for pardon the liberty I am taking.

I am Sir, Sincerely yours
A. W. Kinglake

(BL., Add.Ms. 37205, FF. 81-82).

Lincoln's Inn, April 27

My dear Sir,

I feel very much obliged to you for your most kind offer to apply your own attention to the object of finding the key to the cipher I mentioned.

I well know how valuable your time is, and therefore I think it right that before I venture to trespass upon your leisure for even an instant the utmost efforts of unskilled *labour should be exhausted in the endeavour to apply the partial key which already exists. If, after these efforts, the purport of these papers should still remain in mystery, I will fully avail myself of your kindness & will detail to you some of the strange circumstances surrounding the case.*

I shall be the less reluctant to trouble you since I now know that the family whose feelings are deeply involved in the pending situation have the honour of being personally acquainted with you.

With many thanks, believe me, truly yours
A. W. Kinglake

(BL., Add Ms 37205, FF 83-84)

Lincoln's Inn, July 5, 1854

Dear Sir,

It occurred to me that it might save you some merely mechanical trouble if I were to cause the letters in one of Captain Childe's notes to be counted & distinguished in the way indicated by the accompanying paper

The very great number of times in which the "q" & the "u" are used as finals *will probably give a clue. I also observe that a word written as "sqj" is of constant occurrence.*

I am Sir, most truly yours
A.W. Kinglake

(BL., Add Ms. 37205, F 120)

Figures 4A-C. The Case of Captain Childe

Lincoln's Inn
July 14, 1854

My dear Sir,

I enclose you one of the most important of the cipher letters, & a fac-simile of the writing contained in that letter but (as you desired) with spaces between the lines

You will find a portion of the fac-simile marked at the margin with a pencil, & that is the only part to which (in my reluctance to involve unnecessarily one minute of your precious time) I would venture to ask you to apply the key.

With reference to your wise suggestion as to the expediency of your knowing before hand the kind of way in which your mains would be elicited I would ask you to be so kind as to grant an interview of a few minutes to Mr Gregory the solicitor conducting the investigation on behalf of Mr. Childe, and to one of the Queen's Council of the Common Law Bar who will be professionally engaged for Mr. Childe

The investigation will begin on Monday but the favour of your attendance would not, I believe, be requested until the following day, though I must not say it all would be glad to see you during any period of this curious and somewhat interesting Enquiry.

Most truly yours,
A. W. Kinglake

(BL, Add Ms.37205, FF 121-123).

16 July 1854
Postmark of the original 20 June 1854

Serat [Seraph?] *I have today been informed by the sunary* [summons?] *man here that my letters are in my father's solicitor's hands – and I am hurt and indignated of this further proof of the way in which you art towards mio, and that while you can evidently shew a will of your own on some occasion your own wishes and feelings are more immediate concern. You always shew the most obliging and (to my feelings) mean apathy when you wanted ones wish to do wrong to mio – I will now enter into no arrangement unless your whole government is upset, unless palmerst graham Russel and Aberdeen are all kicked out summarily. I pledge my word I will, if I ever come across any of them, cut them over the ch ps* [chops?] *as I did motan* [maintain?] *– I will enter into no arrangement unless every one of those not only are walked out of office, but all who are members of (the) house of commons cease to be so and unless all cease to appear in public life at all – if you ever ask one of them to your table or house on any occasion I will cease to be anything to you – I insist on russel being walked out of his house in Richmond, I ..st other things. I again repeat to you I will be nothing to you unless I always have a negative free voice on all cabinet appointment and all household appointments – for I am resolved not only that none concerned in confining mio shall come near mio or you – but not even those who associate or consort with the set at all. I will through the whole use or have an entire clearance of all I dislike – clear the course is my word. I will not after this last rascally act put the least restraint on my whims. I have been looking over my maps of black sea. I want to ask you if you are prepared beforehand for what is to be done after Sebast! for I ete* [hate?] *people that look ahead – it appears to me if you mean*

(BL, Add.Ms. 37205, FF. 104-105).

Figures 4D-E. The Case of Captain Childe

7 Gifford St.
July 24, 1854

My dear Sir,

I cannot be satisfied not to endeavour to thank you personally, &, if I should not find you at home, not to do so in writing for the readiness and kindness with which you took the trouble to decypher a portion of my poor son's letters, as well as for your attendance at Clement's Inn during the enquiry.

Alltho' there has not existed in the minds of any member of my family or of the 18 medical gentlemen whom I consulted the slightest doubt of my son's insanity, there might have been considerable difficulty in establishing it to the satisfaction of the jury after the numerous misrepresentations of council and the prevention of a reply by their declining to all witnesses if the decyphered letters had not supplied evidence which appeared to all who heard it quite irresistable.

I am my dear Sir, Very faithfully yours
[..?..] *Childe*

Charles Babbage, Esq.

(BL, Add.Ms. 37205, FF 127-128)

Bedford Square
26 July 1854

My dear Sir,

I should be very much wanting in the proper feeling of gratitude if I omitted to acknowledge the very great service, which I consider to have been rendered to our case on the recent enquiry by the strength of your name and the learned and clear explanation which you gave of the principles by which you had arrived at the certainty of the discovery of the key to the cipher – which at once put an end not merely to doubt but to cavil on the part of our adversaries and triumphantly established the truth of that which I always considered the main strength of our case.

I am well aware that no consideration but those high ones of a regard for the happiness and honour of a most respectable family and a feeling that it was in your person to do a real good would have induced you to give us the assistance of your science and talent as well as of your name on this occasion and I appreciate it accordingly.

I should have written earlier but that since the termination of the enquiry I have not been well and only returned to town yesterday afternoon.

Believe me, My dear Sir, Very truly yours
John S. Gregory

(BL, Add.Ms. 37205, FF 129-130).

Figures 4F-G. The Case of Captain Childe

---

him for an interview the following day together with "*our able council Mr. Montague Smith*", so that together they "*should have the advantage of your personal explanation of the principles on which the science is founded and the certainty to which the discovery is capable of being reduced*".

Inspection of Babbage's solution reveals that the cipher was of a simple type, a so-called *monoalphabetic substitution*, which Babbage had often solved before. That is, the cipher alphabet is produced by a fixed permutation of the conventional

plaintext alphabet such that, for example, plaintext letter "e" is always substituted by cipher letter "w", and similarly for the remaining letters. Hence by this technique the frequent cipher word: "sqj", mentioned in Kinglake's letter of July 5, 1854, becomes but a substitution of the plaintext word: "you". Kinglake's curious observation on the frequency of the cipher letter "q" as a *final* letter, is explained by the fact that the author of the enciphered correspondence, Captain Childe, consistently wrote "mio" in the plaintext rather than "me". A few words, names or phrases of a particularly secret (or frequent) nature do not follow this rule, but are instead represented by a fixed codelist of numbers. Because of their infrequency of occurrence Babbage had to leave these numbers unexplained.

On the worksheet giving the translation of the cipher alphabet, Babbage has jotted down: [16]) "*bad spelling in English; Mistake of cypher Char; Various modes of writing the same cypher Character*". A closer study of the enciphered material[17]) proves this note to be an understatement. Babbage's problem breaking the cipher, was the almost phonetic spelling of the illiterate author and the multitude of enciphering errors. We may all guess that "agen" should be "again" and "imediat" should be "immediate". It becomes more difficult to interpret the wordings: "as moth apposs" by "as much as possible". It would certainly baffle most of us that "Harkosh" is an encipherment error for "Markosh", and hence should mean "My gosh".

But it is not just a matter of spelling. Shuttling between joy and despair, the letters are marked by a strange lack of coherence. The style exhibits but little understanding of the subtle art of suggestion. The good Captain simply writes what in those Victorian days people dared not even think. Truly, these love letters to a member of the fair sex, brings Babbage's remark to the mind, that few ciphers are worth the trouble of unravelling them. It is therefore easy to understand that Babbage, after having read the initial letters, left a major portion in his files without ever bothering to translate it. Still, as these letters provide the only clue as to the parties involved, to the nature of the case, and to the crucial question whether Babbage did in fact appear in court, let me briefly attempt to review their contents selecting some quotations.

Most interesting is perhaps the sketch of the beloved, indirectly painted by Captain Childe. His "*seraph*" is clearly a fallen angel, "*very sweet but very wicked*". Her name is not disclosed, but apparently she is older than he: "*They tell me that you are 35 years old. I don't believe a word of it, because you are definitely just as when I saw you first, not more than 20*". She is known to the public: "*I have just read about you*"; moves in the highest circles of society: "*I don't know if (the) Duchess of Cambridge) know me, but if she does, give my best respects*"; entertains prime ministers and other politicians in her home (see figure 4); and regularly leaves London for the pure country air: "*I am always glad when you are out of the smog*".

For unexplained reasons the relationship has to be kept a secret affair: "*which on my faithful word I do not div(ulge)*". In the strain he becomes more and more possessive: "*I assure you and do beg and beseach, you will not, as far as depends on you, forget what I say or promote what you know I do not like*". Reproached, he promises: "*I will do what you wish. If thy thinks it rite*"; but soon forgets it entering into renewed complaints: "*why do you do these things – you know not how much I dislike them & how much they tend to estrange (me) from you*". Torn by confusion: "*you have said so many strange things to mio. I know not what to think*", or, "*but that cannot be except you have some queer notions – beloved I am sure you have greatly amor mio – but I very often feel as little pleased and satisfied as can be*", he ends up suspended between plea: "*I question that I cannot live with you – to be your lover*" and threats: "*What on earth do you mean? Where is it to end ... you have had warning long ago of what I wished*".

In spite of the indirect references to the ongoing Crimean War (1853-56) and the harsh statements on British prime ministers and other politicians, (see figure 4), the previous quotations seem to indicate personal grievances as the main cause of the law suit, rather than any attempt on his part to use her to meddle in politics.

From the description of the case there can be little doubt that the action is brought against him. Further, the remark in Kinglake's second letter, that he "*now know*" that Babbage is personally acquainted with the Captain's family, seem to imply that the scandal is already out, at least in more well-informed circles. My guess is that she is a well known actress, but here of course I may be entirely wrong. Anyhow, as an open scandal the case could easily expand to involve celebrities or persons of high social status. It therefore had to be handled with circumspection. Indeed, Gregory's repeated reference to "*the strength of your name*" in his last letter to Babbage, and the remark on the adversaries "*declining to all witnesses*" in the letter from Captain Childe's father, should perhaps be interpreted as a result of external pressure.

Before the Judicature Act 1873 a case of this nature was typically falling under the Queen's supreme prerogative of doing *equity* (i.e., right or justice) to her subjects. [18]) This right was exercised through what today is known as the Chancery Division of the High Court of Justice presided over by the Lord High Chancellor. Since Clement's Inn is one of the several Inns of Chancery, this explains that in 1854 it could be the seat of a Court of Equity, even if today all cases are dealt with in Law Courts. Further, since in those days "equity" was considered distinct from "law", a Court of Equity could operate according to rules adapted to the situation.

Combining these facts with those derived from the letters among Babbage's cryptographical papers in the British Library, the conclusion must be that, giving evidence as an impartial expert, Babbage was the key witness in a case brought before a London Court of Equity in 1854. Whether, because of his testimony about

the contents of the enciphered letters, the proceedings were abandoned or compromised on terms, is not known. The fact remains, however, that in *"this curious and somewhat interesting enquiry"*, to quote Kinglake, Babbage made his only public appearance as a professional codebreaker in the service of society.

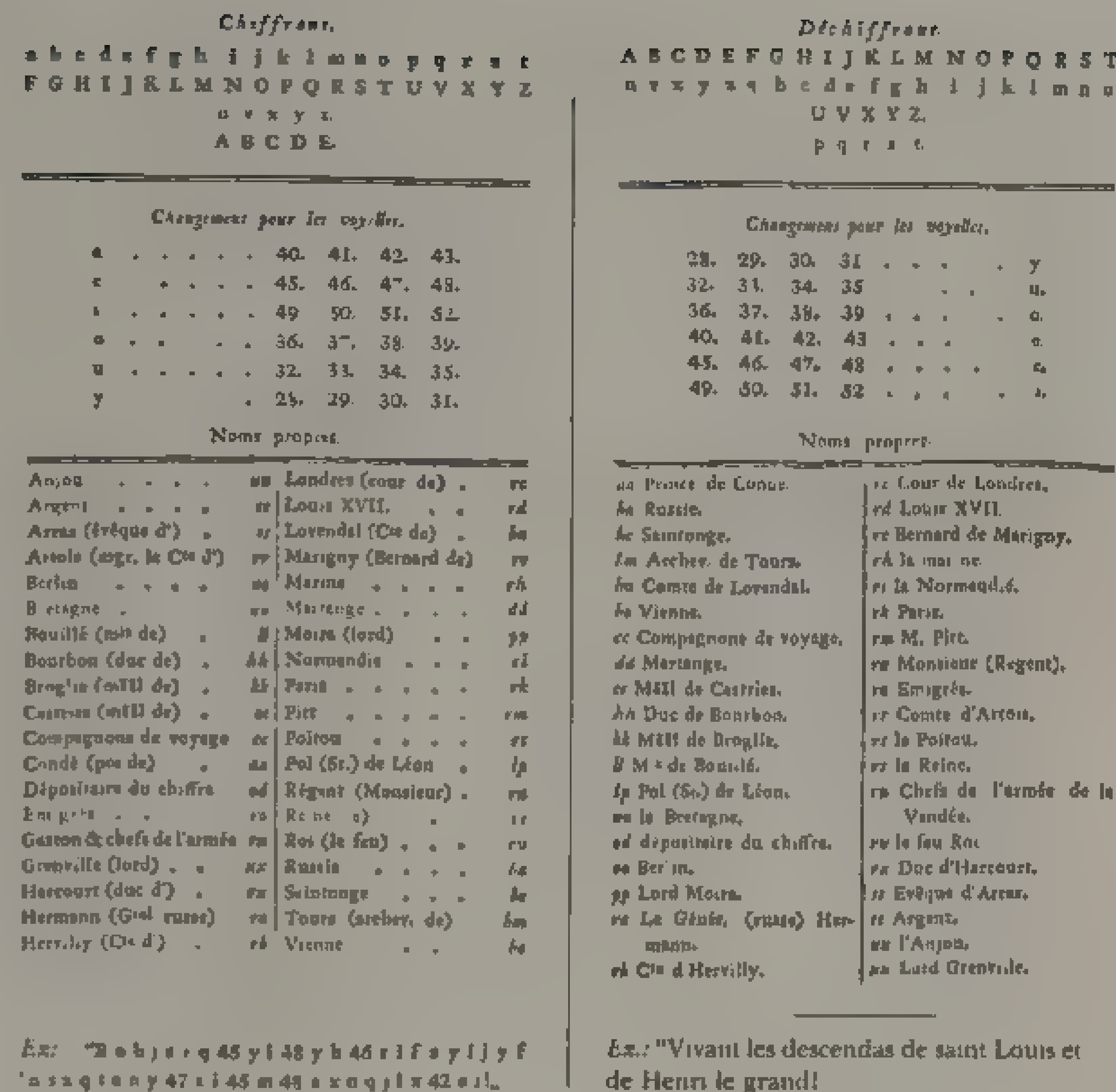
1.3 From Authoritative Sources

The technique of secret writing, half cipher and half code, used in the case of Captain Childe, is known as *nomenclature*. Of course, in direct translation from Latin this term simply means "name-caller", referring in its usual sense to the terminology and thus here to a codelist of names. However, for the period from about 1400 to 1850, say, the term was given this much broader connotation. Further, it was usually implied that the cipher part was a monoalphabetic substitution, while the code part, besides names, encompassed syllables, words, or even phrases as well.

To get an impression of the kind of system Babbage had tackled let us look at simple nomenclature, used by the exciled French princes in the years immediately following the French Revolution in 1789. Described in the first book on cryptography in Danish: *Den hemmelige Skrivekonst*[19] or the Art of Secret Writing from 1819, the author I. B. Lindenfels, a major in the Danish army, introduced it by the words:

> *"The obliging and remarkable goodness of a noble benefactor has enabled the author to communicate to his readers the following cypher, which the Royal French Princes have used during their sojourn in Coblenz and later in the different cities and countries an unfortunate fate forced them gradually to traverse.*
> *This rare document is the much more* authentic *as the benefactor just mentioned has inherited it from his father who not only was one of the correspondents of the Princes, but deeply in their secrets was also a mainspring in the earlier epochs of the counter-revolution, that even his* name *is found* enciphered *among the proper names to be met with in this cypher.*
> *The name, I dare say, is not correctly written, but without doubt, notwithstanding the bad habit of the French more or less to maltreat most non-French proper names, no one will here misunderstand a famous name which, alongside that of Maréchal de Saxe, shines in the temple of immortality."*

This nomenclature, let us call it the Coblenz cipher, is reproduced from Lindenfels' book in figure 5. In a note Lindenfels comments on the cipher from a historical as well as a cryptographic viewpoint. For an officer in a country, which during the Napoleonic wars had been forced from a state of neutrality into an unhappy alliance with France, Lindenfels discloses here and elsewhere in his book a rare,



Chiffreur.

a b c d e f g h i j k l m n o p q r s t
F G H I J K L M N O P Q R S T U V X Y Z
u v x y z.
A B C D E.

Changemens pour les voyelles.

a	40.	41.	42.	43.
e	45.	46.	47.	48.
i	49	50.	51.	52.
o	36.	37.	38.	39.
u	32.	33.	34.	35.
y	28.	29.	30.	31.

Noms propres.

Anjou	uu	Londres (cour de)	rc
Argent	tt	Louis XVII.	rd
Arras (évêque d')	ss	Lovendal (Cte de)	bn
Artois (mgr. le Cte d')	rr	Marigny (Bernard de)	re
Berlin	oo	Marine	rh
Bretagne	mm	Martange	dd
Bouillé (mis de)	ll	Moira (lord)	pp
Bourbon (duc de)	hh	Normandie	ri
Broglie (mll de)	kk	Paris	rk
Castries (mll de)	cr	Pitt	rm
Compagnons de voyage	cc	Poitou	rs
Condé (pce de)	aa	Pol (St.) de Léon	lp
Dépositaire du chiffre	od	Régent (Monsieur)	rn
Emigrés	ro	Reine	rt
Gaston & chefs de l'armée	ru	Roi (le feu)	rv
Grenville (lord)	xx	Russie	ba
Harcourt (duc d')	rx	Saintonge	bc
Hermann (Gal russe)	ra	Tours (archev. de)	bm
Hervilly (Cte d')	rb	Vienne	bo

Ex: "B o b j e r q 45 y i 48 y b 46 r i f s y i j y f 'n s x q t e n y 47 x i 45 m 48 x x o q j i x 42 e s !.

Déchiffreur.

A B C D E F G H I J K L M N O P Q R S T
u v x y z a b c d e f g h i j k l m n o
U V X Y Z.
p q r s t.

Changemens pour les voyelles.

28.	29.	30.	31	y
32.	33.	34.	35	u.
36.	37.	38.	39	o.
40.	41.	42.	43	a.
45.	46.	47.	48	e.
49.	50.	51.	52	i.

Noms propres.

aa Prince de Condé.	rc Cour de Londres.
ba Russie.	rd Louis XVII.
bc Saintonge.	re Bernard de Marigny.
bm Archev. de Tours.	rh la marine.
bn Comte de Lovendal.	ri la Normandie.
bo Vienne.	rk Paris.
cc Compagnons de voyage.	rm M. Pitt.
dd Martange.	rn Monsieur (Regent).
cr Mâll de Castries.	ro Emigrés.
hh Duc de Bourbon.	rr Comte d'Artois.
kk Mâll de Broglie.	rs le Poitou.
ll Mis de Bouillé.	rt la Reine.
lp Pol (St.) de Léon.	ru Chefs de l'armée de la Vendée.
mm la Bretagne.	rv le feu Roi.
od dépositaire du chiffre.	rx Duc d'Harcourt.
oo Berlin.	ss Evêque d'Arras.
pp Lord Moira.	tt Argent.
ra Le Génér. (russe) Hermann.	uu l'Anjou.
rb Cte d'Hervilly.	xx Lord Grenville.

Ex.: "Vivant les descendas de saint Louis et de Henri le grand!

Figure 5. Enciphering and deciphering by the Coblenz Cipher (Lindenfels, 1819)

almost personal dislike of the French Revolution. Referring to the Coblenz cipher as *"a kind of special document in the history of the French Revolution"*, he thus declares that *"everybody who favours a successful outcome of this bloody tragedy, will in this secret act*

have the pleasure of meeting again the names of those tried and loyal subjects who ever, under all circumstances, proved themselves zealous defenders of the rightful government". He continues that those knowledgeable of the Art of Ciphers, will find in this cipher additional proof of the claim in his preface, that evil persons will always find far more means of doing harm, than noble and unsuspecting people could ever imagine to prevent it. In short, the "*cipher alphabet of the princes is to that degree innocent, simple and naive that it hardly can be considered a cipher*". Although Lindenfels disguised his book as entertainment, he clearly had a message to his countrymen.

The Coblenz cipher, as Lindenfels pointed out, is no more than a trivial variation of a cipher used by Julius Cæsar, Emperor Augustus, Cicero, and Seneca among others. Giving exact references with quotations in Latin he rapidly traces its history adding, tongue in cheek, that "*the grammarian Probus should have found it worth the trouble to write a complete treatise on Cæsar's ciphers.*" As the reader may verify, the cipher alphabet, known today as a *Cæsar alphabet*, is but a fixed cyclic shift or rotation of the plaintext alphabet. Hence, it is solved automatically, trying all the possible rotations of the alphabet. This technique which later will be demonstrated in APL, is known popularly as "*running down the alphabet*". The additional variation of introducing various 2-digit numbers for the vowels, provides little or no complication at all, since the vowels may always be guessed if all the consonants are known. Accordingly, the only problem of this cipher is to establish from the context or other information the proper names hiding behind the 2-letter code

Another far more difficult nomenclature described by Lindenfels in a postscript to his book, is a diplomatic cipher of Anthon W. von Haxthausen, envoy of the Danish King Christian IV (1577-1648) to several foreign courts. Reproduced from Lindenfels' book in figure 6, the plaintext alphabet, as the reader will observe, is represented by no less than five different, somewhat randomly permuted cipher alphabets in terms of 1- and 2-digit numbers. The use of a given of these cipher alphabets is signaled by a preceding 1- or 2-digit number which, called an *index* or a *changer* sign, is selected out of three possible for each alphabet. Further, interspersed into the text are numbers void of meaning, the socalled *nulls* or, as Lindenfels calls them, *non-valeurs*. Elsewhere he mentions that, in addition to the latter, such ciphers may also contain numbers assigned to special indicators, the *contresens*, which changes the meaning of a statement to its opposite.

Lindenfels recounts that this cipher too was sent to him by the benefactor contributing the Coblenz cipher. Together with a similar cipher it was contained in a sheaf of original documents marked on the cover: "*Chiffres du Gr. Ecuier Anthon W v. Haxthausen dans ses mission á differentes Cour*". Presumably, as indicated by his title: "Grand Ecuyer" or Master in Chief of the Horse, von Haxthausen must have been on special missions reporting directly to the King. Chances are therefore that,

Chiffre chiffrant et déchiffrant.

In-	di-	ces.	+	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	V	Z	O
11	13	9	+	17	1	18	21	2	22	3	23	24	25	7	4	16	19	20	26	27	28	29	38	39	40	41	42
30	34	36	+	19	20	1	2	3	4	5	16	7	8	29	43	44	6	49	46	47	48	49	50	54	53	52	51
35	12	37	+	16	17	19	18	20	21	22	24	23	26	25	5	6	7	8	39	38	37	36	5	4	3	2	1
14	32	33	+	1	2	3	4	5	22	23	26	27	28	29	40	39	39	24	21	20	19	18	17	16	8	7	6
31	10	15	+	41	43	45	47	49	51	53	55	57	59	60	61	62	63	64	58	56	54	52	50	48	46	44	42

"Alle tal fra 1 til 64 ehre Alphabetisk; inclusive fra 64 til 100 Betyder de Inted, men settes "Vndertiden imelum att giøre Vdtydningen des wanskeliger. Fra 100 til 186 betyder de Steders "Naffne." — —

"Alle tal fra 8 til 16 Exclusive och fra 29 til 38 ochsaa exclusive ehre Indices saaledes att "forat forandre Bogstaffuerne att Andre dett Ey kand Dechiffrere, bruges vndertiden denn Ene "Raad Tal vndertiden den Anden och settes altid en aff indicibus aff samme Rad for, for "Exempel Kongens Tittel,,

"C h r i s t i a n u s q u a r t ■ s
"11. 18. 23. 27. 24. 28. 29. 30. 7. 19. 44. 50. 48. 46. 35. 5. 16. 38. 36. 32. 17. 18.
"d e i ■ r a t i a ■ ■ n i e n o r u ■ g i
"4. 5. 27. 23. 20. 1. 18. 31. 57. 41. 13. 21. 17. 16. 24. 2. 34. 44. 6. 47. 50. 3. 5. 7.
"e u a n d a l o ■ ■ m ■ o t o r u-
"37. 20. 5. 16. 6. 18. 14. 1. 29 38. 20. 17. 40. 9. 3. 19. 29. 36. 6. 47. 34. 50.
"m q u e r e x"
"43. 46. 13. 38. 2. 27. 31. 49. 48.."

Figure 6. Haxthausen's diplomatic cipher (Lindenfels, 1819)

Translation: "All numbers from 1 to 64 are alphabetic, (all) inclusive from 64 to 100 mean nothing, but are now and then interspersed to make the breaking the more difficult. From 100 to 186 they mean names of places ... All numbers from 8 to 16 exclusive and from 29 to 38 also exclusive, are indices so that, to change the letters that others cannot decypher it, sometimes one row of numbers and sometimes another row of numbers is used, always preceded by one of the indices of the same row, for example the King's title

Christianus quartus dei gratia danie norvegie uandalorum gotorum que rex" (i.e., Christian IV, by Grace of God, King of the Danes, the Norwegians, the Wends, and the Goths)

Figure 7. Rundetårn (The Round Tower) in Copenhagen, built 1637-42 by Christian IV as an astronomical observatory for Tycho Brahe's student and faithful assistant Longomontanus. Later used by Ole Rømer, the discoverer of the finite velocity of light. A drawing made by the King himself of the rebus [20]) ornamenting the outer wall, is preserved in Rigsarkivet (The State Record Office). An erratic composite of Latin, Hebrew and carved figures it should be read: "Faith (DOCTRINAMET) and Justice (the Sword) is Directed (DIRIGE) by the Lord (JEHOVA, written in Hebrew) into the Heart (depicted in red) of the Crowned (the Crown) Chr. IV (the Monogram) 1642". However, in the Copenhagener wit the interpretation has always been "The doctor with the long knife directs scribble-scrabble into the heart of Chr. IV 1642" (Photograph, courtesy Nordisk Pressefoto)

with his keen interest and brilliant understanding of all kinds of engineering problems, Christian IV selected the cipher himself (see figure 7). Anyhow Lindenfels claims that, even if the documents are somewhat "*moth-eaten*" and difficult to read because of their venerable age, every care has been taken to produce an exact replica. To anyone familiar with the Danish language this explains its archaic spelling and wording which I had to forego in the English translation.

The cipher is used together with a nomenclature or, as Lindenfels frequently calls it, a *passe-partout*, divided into two parts. The numerical part, consisting of the numbers 100-186, is but a list of geographical places. The other part, entitled "*Prouincier och Dignitates*" (provinces and dignitaries), comprises slightly more than one hundred alphabetic entries denoted symbolically by a set of "*curious signs*". He remarks that diplomats of today (1819), would probably frown upon the latter nomenclature because of the additional labour incurred.

The problem of printing a special character set, is also what prevents him from presenting in his book the other cipher contained in these documents. However, since its two-part nomenclature differs from that of the former cipher he briefly discusses it. The numerical part is a list of 3-digit numbers assigned to the names of persons at the Danish Court and abroad, while the alphabetic part is a dictionary of frequent words in French. Life at court in the late 16th century, is revealed in a glimpse by Lindenfels' choice quotation from this dictionary: "*Bassette, berlaud, boire, banquet, cartes, caffé, chocolate, collation, ducats, &c*" (Name of a game, chatterer, drink, banquet, playing cards, coffee, chocolate, refreshment, ducats, etc.).

To contrast the inferior state of secret writing, as documented in his own time by the Coblenz cipher, Lindenfels points out that, even if more than a couple of centuries old, the Haxthausen cipher may still be applied to brief dispatches. Indeed, says he, it was employed in the same fruitful period as that in which Vigenère described his cipher; and clearly, the two ciphers are related. Because in either case, the aim is to enable the user to substitute alternative cipher letters, in the course of the text, for one and the same plaintext letter. Since this is achieved introducing several cipher alphabets according to a rule (a key), they are classified today as *polyalphabetic substitution ciphers*.

The authenticity of the Coblenz and the Haxthausen ciphers is vouched for by the name: "*Comte de Lovendal*", listed in the nomenclature of the former cipher (see figure 5). A misspelling of the name Løvendal (Lionvalley) we immediately recognize, by its reference to the lions in the coat of arms of the Danish king, a lineal descendant of a royal mésalliance. [21]) The ancestor of this family branch was an illegitimate son of King Frederik III, Ulrik Frederik Gyldenløve (1638-1704), who, true to his name (Goldenlion), made his imprint on the war history of Northern Europe as Danish Field Marshal and Viceroy of Norway.

However, in Danish literature he merely performed as a supernumerary, being the first husband of Marie Grubbe. The enigmatic nobleman's daughter who, during her second marriage to a squire, eventually ran away with the coachman to end up as a ferry woman on Falster, where she pulled the oars herself after her husband in 1711 had been arrested for murder. The passion, the social disgrace, and the resignation of this fascinating female character, were originally described by the father of the Danish-Norwegian theatre, the playwright Ludvig Holberg, who as a young student took refuge in her ferry-inn from the plague in Copenhagen, and thus had the opportunity to "interview" her. Later, her fascinating fate was immortalized by three other great Danish poets: Hans Christian Andersen, J. P. Jacobsen, and Steen Steensen Blicher.

The grandson of Gyldenløve in his first marriage to Sophie Urne, was François Xavier Joseph Count Danneskiold-Løvendal (1742-1808), the owner of the Coblenz cipher. Brought up in France, he was commissioned in the French army, participating as a colonel in the Seven Years War. Promoted brigadier in 1771, he served under Marquis de Lafayette in the American War of Independence commanding the Armagnac regiment. For a couple of years he was then commandant on Guadeloupe before he was recalled in 1779 and promoted Maréchal de camp. After the French Revolution, he entered the emigrant army serving under the Prince of Condé who, as one will notice, is also listed in the nomenclature of the Coblenz cipher. He came to Denmark in 1795 where he was commissioned as major-general and given the command of the Marine Corps. In 1801 he entered diplomatic service, serving first as Danish Ambassador to the Imperial Court in St. Petersburg and, from 1803 to his death, as Danish Ambassador to the Batavian Republic in The Hague.

These few facts about Count Løvendal's professional career not only establish the truth of Lindenfels' account, but also throw into relief the prostrate admiration emerging from his description. Yet, most important of all, they provide the necessary background for a story of Lindenfels's benefactor, no less fascinating than that of Marie Grubbe.

Carl Woldemar Count Danneskiold-Løvendal (1773-1829) who had a French mother, was brought up in Versailles and Paris where he studied at Collège d'Harcourt. In 1787 he was commissioned in the French army, joining the emigrant army together with his father after the Revolution. Following his father to Denmark in 1795 he entered the Royal Life Guard as a lieutenant. In 1801, travelling as courier with dispatches from the King to his father in St. Petersburg, he lost the dispatches in Åbo, Finland, which was then part of the Russian Empire. Protected by his name he got away with three months imprisonment in the Citadel of Copenhagen. In 1807, he was promoted captain and company commander of the chasseurs of the Danish Life Regiment, a new regimental elite unit of 150 grey-jacketed marksmen which had been introduced by Frederik VI inspired by the accomplishments of the American militia in the War of Independence. [22])

In 1813, being promoted major, he was ordered to serve in Hamburg at the headquarters of Napoleon's Marshal Davout, under whom the Danish Auxiliary Army Corps was placed. For some reason or other the Marshal imprisoned Løvendal for four months. Released, he went back to his command of the chasseurs, although simultaneously he was ordered to serve also in the artillery which was then rapidly developing into a fast-moving, offensive core. It was during this period that he communicated the historical ciphers to Lindenfels.

A naturalized Dane with French as his mother tongue it is not surprising to

find, as quoted by Lindenfels, that Løvendal's covering letter for the Haxthausen cipher was in this language. Dated 23 March 1819 it opened: "*J'ai découvert aujourd'hui dans les papier de la famille Haxth. les* deux chiffres *que je vous envoie, Monsieur le Major; quoique* tard *ils vous seront peut-être utiles ...etc.*" (I discovered today among the papers of the Haxth. family the *two ciphers* which I enclose for you, Monsieur le Major; somewhat *late* they may perhaps be of use to you ...etc.). Apart from this statement Lindenfels provides no clue explaining how or why Løvendal happened to come across the Haxthausen papers.

Brilliantly educated by the standard of those days, Løvendal undoubtedly was a man of many-sided cultural interests. So perhaps we may imagine that, like many of his brother officers on the borderline of sheer poverty, he used his skills and knowledge to supplement his income. To be sure, officers of the lower ranks were in fact forbidden to marry, unless either they had private capital or the marriage would "*considerably improve their financial circumstances*".

Løvendal retired with the rank of lieutenant-colonel in 1828 and died the following year, as the chronicler said, "*from neurasthenia*". The social disgrace of his imprisonments, his relatively low status in the army, and his lack of money undoubtedly closed to him that part of society which matched the obligations of his name. He therefore died unmarried because he found that "*it was better to let our name die out than transmit it to children who like us would have to fight poverty and adversity*". Still, before his death Frederik VI allowed that his name and title might be inherited by his sister's son Rutger Bangemann Huygens.

Nothwithstanding this depressing end there is a droll point to our story. For in the calendar of the Danish nobility I found that he left behind four bastard children by three different women. In 1805 a son by Lehne Dorothea Poulsen. In 1813 a daughter and in 1818 a son, both by Anne Kirstine Svane, daughter of a journeyman smith. This second mistress must clearly have been unmarried, because to protect her he succeeded in 1817 to obtain for her the right that she might call herself "*Widow Anne Kirstine Svane*". In the intervening period between the two children they apparently had a disagreement, because in 1816 he had a daughter by an "*unknown mother*". This curious statement is explained by the fact that, at the maternity hospital in those days, an expecting mother who desired to remain anonymous, was given the option of being registered only by a serial number.

It is comforting to report that Løvendal did not abandon his four children. In fact, petitioning Frederik VI who was a very human and compassionate ruler, Løvendal contrived that all four were granted the rights of a noble birth and, as his legitimate children, were entitled to adopt the name Løvensøn (Lionson).

1.4 Royal Correspondence

In the preface to his *Passages* Babbage remarked that *"a list of my works ... formed the best life of an author"*. Yet, as perceived by posterity he fell short of this measure. This, however, was far from the intentions he happened to reveal in 1858 in the correspondence with a Mrs. Everett Green. [23])

From the transcript of this correspondence, given in figures 8A-C, it will appear that Babbage's proposed work on ciphers was planned to be a book entitled *"The Philosophy of Decyphering"*. Further, we are informed that he was considering to use as illustrations for part of the book some material on a cipher of Charles I.

The work Mrs. Green accepted as *"a memorial of your indefatigable labours"*, I would suggest, was Babbage's solution of a related cipher. Because, among his cryptographic worksheets on these historical ciphers, there is but one solution of his own. Namely, as he has written on its title page [24]): *"Letter of Henrietta Maria, Queen of Charles I, deciphered by C. B., July 1858"*. [25]) What better gift to present to a lady of such professed interest in the ciphers of Charles I.

Babbage's careful historical studies, undertaken in preparation for solving these ciphers of Charles I and his Queen, are disclosed in the undated draft of an incomplete letter transcribed in figure 9 (see page 36). Judged from his worksheets, the four step procedure outlined in this letter, appears to be the one he himself followed. But before I go into more detail on this, the casual reference to the contents of his book on deciphering should also be noted. As far as I have been able to ascertain, his remaining scientific papers on deciphering in the British Library contain no further references to this work. It is time therefore, briefly to sum up the few facts we have been able to establish about his plans for this contribution.

In the letter of 8 December 1857 (see figure 1) he claims that *"the object of my proposed work on cypher is not exactly what you suppose"*. A statement which I have interpreted to mean that, rather than a popular account, he intended to write a scientific treatise. This hypothesis is substantiated by the remark in his letter of early August 1858 to Mrs. Everett Green, disclosing that the proposed work was a *"book"*, tentatively entitled *"The Philosophy of Decyphering"* (see figure 8B). The unfinished draft of the letter on the ciphers of Charles I, presumably also written in August 1858, further corroborates this observation (see figure 9). The last mentioned two letters each gives a fact about the intended contents of this book.

(1) The researches of Mrs. Green on the ciphers of Charles I supplied *"valuable illustrations for some portions of* [the] *work"*

(2) *"Extensive lists of all words of English language arranged in classes"*, were prepared as material for the book.

Dear Sir,

My keys do not read either of your cyphers in my hands. I question that they will do better in yours – but if you will excuse the very rough manner in which they are got up, I enclose them, because they will just give you an idea of the general plan forming the cyphers. They are so rough as to be scarcely intelligible but to myself, only that I can say they will not baffle you. I shall be most interested to know whether your efforts prove successful. I am, dear Sir

Yours faithfully
Mrs. E. Green

7 Upper Gower St.
July 31/58

A) BL, Add Ms. 37205, FF 209-210

My dear Madam,

I have kept the cypher keys you so kindly lent me longer than I had intended owing to the very few hours I can spare from my other pursuits for the fascinating one of decyphering. I had previously at the Museum made out much of two of the cyphers, but my extracts were rendered more complete by add: from yours

I have no doubt that the letter of Ch II can be decyphered, but it may be at the expense of months to any not familiar with the history of the time. I can not attempt it in the regular way but am not sorry that my attention has been called to the subject – since your researches have supplied me with valuable illustrations for some portions of work in the Philosophy of Decyphering if I should ever have time to write that book

In the mean time allow me to offer you a work on another subject which accompanies this note.

I am, My Dear Madam
Yours truly
C B

B) BL, Add Ms. 37205, F. 211

My dear Sir,

On returning from a month's sojourn in the country I find your kind note and present – Pray accept my cordial thanks for such a memorial of your indefatigable labours, which I shall value the more as presented by yourself

I understood the cypher letter was from Charles I, but your last note says Charles II. In that case there was a chance of my cypher proving available.

With much respect I am, dear Sir,

Very truly yours
Mrs. Everett Green

7 Upper Gower St.
Aug. 30, 1858

C) BL, Add Ms. 37205, FF. 212-213

Figure 8. The correspondence with Mrs. Everett Green

My dear sir,

I am so completely occupied by the construction of the Analytical Engine that there is no probability during the next two years of my finding any time to devote to a difficult cypher.

I have prepared extensive lists of all words of English language arranged in classes as material on the philosophy of deciphering to which, on rare occasions, I give half an hour as relaxation from my daily labour

There are I apprehend many letters in cypher of the time of Charles the First which have been decyphered and are printed.

1st A list of where should be made with references to the books in which they occur

2 From these letters all english words should be extracted whose mode of spelling is different from that at present used.

3 These should be arranged in their several classes

4 The date of the letter, the place where it was written, that of the person to whom addressed, as any conjecture as to the nature of communication should be stated

Figure 9. Incomplete draft of letter to an unknown (BL, Add MS. 37205, F 214)

Since the latter point will be dealt with in part three, let us here concentrate the interest on the former.

How Babbage got interested in these historical ciphers, is not at all clear. Yet it is evident from his notes that he did some research on the original manuscripts in, what he refers to as, the Harleian Collection in British Museum and the State Paper Office. [26]) The dominant part of his notes and worksheets relates to the four-step procedure outlined in his incomplete letter (figure 9), leaving to the imagination of the reader how he actually went about solving the cipher used in the letter of Henrietta Maria

On his transcript of this letter, double-spaced to give room for the solution, Babbage has identified the original by the reference: "*No. 7379 Harl. Mss. Br Mus. folio 32*". With the plaintext written in French it is enciphered by a simple monoalphabetic substitution, represented by 2-digit numbers, and rather sparingly interjected with 2- and 3-digit code numbers. In short, it is the same type of nomenclature as the Coblenz cipher, but with a better randomization of the cipher alphabet.

From Babbage's translation it would seem that it is dated "*Paris, 4 Feb.*", although the year is not given. In the margin, apparently at a later point in time, Babbage has scribbled: "*At fol. 32 part of another letter dated Paris, Decem. 8 or 9. written partly in English in s a m e cipher, there appear several triplets translated as below*" Among the translations of "triplets" or 3-digit code numbers listed by Babbage we find not only names of persons (*140. Digby: 245: P.Or*, the Prince of Orange), places

(*145.England; 184-185. Holland*) and cities (*155. Edinb.; 255 Paris*), but also frequent words, both general (*416. here; 318. his; 420. her*) and more special (*324 armes; 482. Parliament; 488. powder; 506 rebells*) in addition to a few phrases (*448.330.324.547.220*, meaning *money. and. armes. to. His Majestie*). On a separate worksheet Babbage has organized this incomplete nomenclature in numerical order for use in deciphering.

It will be recalled from history that a daughter of Marie de Médicis, Henrietta Maria, took refuge in Paris with her brother, Louis XIII of France, during the civil war. From there she carried on a voluminous correspondence in cipher. For example, in January 1647, while still in the hands of the Scots after the fall of Newark, Charles I wrote the Marquis of Montrose, the "*noble character and brilliant general*" as Sir Winston Churchill called him, that for want of a cipher he would have to refer him to the Queen for instructions. Montrose who had been ordered by Charles to disband his forces and repair to the Continent, received the letter in Hamburg on his way to seek audience with Christian IV of Denmark who had always been a staunch friend to his nephew Charles I. Delaying his stay in Hamburg, Montrose finally received the long awaited letter from Henrietta Maria in early February. [27])

According to Babbage's notes on the Queen's letters he found, by examination of "*90 folios*" of this correspondence in British Museum, that she changed ciphers and associated nomenclature four times over the period from March 1642 to April 1645. From Babbage's description of the first three of these ciphers (the fourth he left undescribed), we see, how the experience of their use in practice influenced their design.

In the first cipher, used March-August 1642, the "*alphabet* [is] *enciphr'd by figures and symbols*, [and the] *small words by* [a] *combination of fig's and letters.*"

In the second cipher, used until the spring of 1643, the representation is numerical except for the code of smaller words, "*in which the compound of figures and letters used in the first are repeated occasionally*". Apparently, each plaintext letter is given alternative numerical cipher representations, simultaneously as the code part is extended considerably. Wrote Babbage: "*The single letters and blanks occupy from 1 to 77. The higher numbers up to 339 are devoted to proper names which follow each other in Alp*[habetica]*l sequence as to initials only*".

In the third cipher, used until April 1645, the last trace of letters has been removed, so that the representation is now entirely numerical. According to Babbage this cipher is "*more comprehensive than the former* [and] *includes a large range of words* [and] *parts of words in frequent use. Single letters and blanks occupy numbers to 80, thence to 322 names of persons and places. Upwards as high as 574 words of frequent occurrence.*"

A few additional notes, dropped here and there across the worksheet containing this description of Henrietta Maria's three ciphers, suggest a plausible explanation of the puzzle surrounding Babbage's work on the Queen's cipher. On the top of the page he has written *"Keys compiled from the deciphered passages"*. Below this description of the second cipher he has added that it was *"used until spring of 1643 and afterwards with the Duke of Newcastle. Much of the original in the Harl. Mss."*. And finally in connection with the third cipher he has stated: *"The originals of these letters exist in the state paper office and have materially assisted in the formation of the key as they are all carefully deciphered"*, adding in a separate note in the margin: *"3rd cipher a sheet of figures"*.

As I interpret these clues, it would appear that Babbage in 1858 examined these royal letters in British Museum in order to establish from the deciphered passages the nomenclatures actually used. This provided him with the first and the second cipher. However, they did not work for a sheet of figures (being the third cipher) of which he brought home a transcript that he partly cracked. This was the letter in French dated *"Paris, 4 Feb."* of, what must have been, the year 1645. Afterwards he discovered in the state paper office the deciphered letters in English which permitted him to reconstruct also the third nomenclature or key as he called it.

The nomenclatures or ciphers of Charles I which Babbage obtained from Mrs. Green, seem to be preserved among his papers in the form of transcripts. A typical illustration, is what Babbage designates· the second cipher used by Charles I to the Earl of Arundel in Flanders 1636. [28]) The cipher part is a monoalphabetic substitution with all alphabetic letters substituted by 2-digit numbers, such that there are two alternative number representations for each consonant, four for each vowel, eight for the nulls, and only one for each doubling of a letter. The code part is a list of 3-digit numbers, containing the type of information already described in connection with the related ciphers of Henrietta Maria. In fact, the only addition seems to be that the code list now also contains the number of the month and all dates from the first up to the thirty-first.

In principle all the ciphers of Henrietta Maria and Charles I fall into the same category as that of the Coblenz cipher. Although better randomized and more elaborate in the sense that a plaintext letter may have alternative cipher letter substitutes, they all suffer from the same defect. Namely, that a given cipher letter (number) uniquely identifies one and the same plaintext letter throughout the text. It is this defect which the contemporary Haxthausen cipher attempts to remedy.

With the pattern of these ciphers well established it is easy to understand that Babbage felt no urge to accept the challenge of solving one of Charles I's ciphers (see figures 8 & 9). The physicist Charles Wheatstone was therefore approached and, accepting, he succeeded. This story, published less than twenty years after the

event by W. T. Jeans in his *Lifes of the Electricians* from 1887, is not only of interest in itself. It also adds perspective to Babbage's correspondence on the ciphers of Charles I. Recounted Jeans: [29])

> *A marvellous instance of his skill in deciphering cryptographic documents occurred in 1858. Sir Henry Ellis relates that a good many years previously the trustees of the British Museum purchased at a high price what appeared to be a very important document in cipher, occupying seven folio pages closely filled with numerals. The top of every page bore the signature of King Charles the First, and was countersigned by Digbye. For a long time Sir Henry Ellis endeavoured to get it deciphered for the purpose of including it in his series of letters illustrative of the history of England, but he could not get any one able to read it. One evening at Earl Stanhope's he accidently mentioned that fact to Lord Wrottesley, who suggested that Professor Wheatstone's ingenuity might be able to unravel the secret writing, and accordingly Sir Henry Ellis at once sent it to the Professor, requesting that he would investigate its contents. This took place on June 1st, 1858. In the document in question about ninety different numerals were employed to represent the letters of the alphabet, and besides the complexity of each letter being represented by several distinct numerals, there was no division between the different words, and the numbers represented not English (as was as first supposed) but French words. This document, which had baffled all other experts, was interpreted by Professor Wheatstone. A copy of it having been sent two or three years afterwards to the Philobiblion Society, along with the key to the cipher, the Society expressed "their admiration of this additional instance of that wonderful faculty of interpretation which seems to ordinary minds a special intuition not unworthy of a great scientific discoverer and practical benefactor of the age".*

Somewhat disappointingly the letter turned out to be a marriage contract. The solution together with Wheatstone's explanation of the key was published in 1862 in the *Memoirs of the Philobiblion Society.* [30]) May we guess that the unknown gentleman, inviting Babbage to do the job, was in fact Sir Henry Ellis himself?

1.5 From Babbage's Library

The first perusal of Babbage's scientific papers *"On cyphers and decyphering"* [2]) in the Manuscript Room of British Library, will probably deter most investigators. Page after page of draft computations, records of alphabetic letter counts, formulas, hasty translations of ciphers, newspaper clippings, letters, etc., in great disorder (except for an arbitrary, but not always chronologically correct, ordering by folio numbers), but no trace of any explanation, not to say a list of contents or a manuscript, giving evidence of his *"proposed work on cypher"*. Of all the papers Babbage left behind him, this collection is truly the most cryptic.

David Kahn, after having studied Babbage's papers, wrote in his fascinating historical account *The Codebreakers* from 1967 [25]): "... *His papers are filled with formulas which he used to help him solve ciphers and see their underlying structure more clearly. Unfortunately his notes are too scrappy and incomplete to give any more than a tantalizing glimpse of what he was trying to do*". Whether Kahn on this occasion had taken notice of the scattered remarks on the proposed work on ciphers in Babbage's letters, is not clear from his account. But in the course of his discussion on how to break a cipher developed by Wheatstone, he puts forward the intriguing suggestion that "*an extremely perceptive article signed only "C.P.B." and published in MacMillan's Magazine*" in 1871, might have been written by "*Charles Babbage, though elsewhere he never used a middle initial*". [31]) The question therefore arises whether this anonymous article could perhaps be part of Babbage's manuscript for the Philosophy of Deciphering?

For various reasons of which I shall give a few, it appears reasonable to conclude that the answer must be in the negative. The first initial in the signature of the article is not "C" for Charles, as quoted by Kahn, but "G", perhaps for George. Babbage had no middle name. In the baptismal register at St. Mary Newington, as established by Hyman [4]), there was recorded for 6 January 1792: "*Charles, son to Benjamin and Betty Plumleigh Babbage*".

In view of the repeated references to the proposed work on ciphers in his various letters, often to complete strangers, it appears highly unlikely that Babbage should publish this work, or parts thereof, anonymously. After all, in his *Passages* from 1864 he even acknowledged his authorship of the anonymous letters on Mr. Thwaites' cipher in the Journal of Society of Arts ten years earlier.

In a recent article, published in 1981, M. R. Williams [32]) described his accidental discovery of Babbage's private mathematical and scientific library, which has been kept intact and is now part of a larger collection, called the Crawford Collection, in the library of the Royal Observatory in Edinburgh. A catalogue, prepared in 1872 by R. Tucker for the sale of this library, lists more than 2500 titles on, in particular, mathematics, physics, astronomy, and tables of all forms. [33]) A perusal of this sales catalogue will show that Babbage used to file copies of his own publications in this library. The MacMillan paper, however, is not listed in the catalogue.

If this paper had been listed in the catalogue it would have been an observation of value. The opposite is not the case. In his article Williams recounts that after Tucker had prepared the catalogue, "*the family withdrew 58 items from the collection, leaving 2529 items offered for sale*". Evidently the family could as well have removed items of interest before the preparation of the catalogue

Williams estimates that Babbage was most active in building up his collection between 1820 and 1830, by which latter year he had obtained over 60 per cent of

his entire holdings. As even a quick glance through the catalogue will reveal, Babbage's collection is impressive. It comprises the original editions of the works of nearly all of the great names in the mathematical and physical sciences since Galilei. Yet, even if famous cryptographers like Giovanni Battista della Porto, Girolamo Cardano, Francis Bacon, Francois Viète, and John Wallis are amply represented by their mathematical contributions, the catalogue lists only two books on cryptography.

One, entitled *De reticulis cryptographicis*, was published 1799 in Leipzig by Maurice de Prasse. The catalogue lists eleven other works by de Prasse, all on mathematics and all printed in Leipzig. Chances are, therefore, that they belong to the lot purchased by Babbage, visiting the "*book fair in Lepsic*", as he remarks in his *Passages*. I have failed to find further information on de Prasse's cryptographical publication. Still, the title suggests a network type cipher, perhaps the grille invented by Cardano.

A *grille* is a sheet of stiff material (e.g., cardboard) in which holes are cut on purposeful positions. The secret message is read through the holes, when the grille is properly placed over some inconspicuous text into which the hidden message has been written. According to Kahn a number of countries made use of the Cardano grille in their diplomatic correspondence in the 16th and 17th century. Babbage's contemporary, William Makepeace Thackeray, uses one in his famous historical novel: *The History of Henry Esmond, Esq. – A Colonel in the Service of Her Majesty Queen Anne*, published in 1852. It is well known that, prior to writing this novel, Thackeray undertook an intensive historical study of the files of those days in British Museum.

The other work listed in the catalogue of Babbage's library, is the 1802 edition of the collected works of Bishop John Wilkins. [34]) This edition includes Wilkins' classical treatise from 1641: *Mercury, or the Secret and Swift Messenger. Shewing how a Man may with Privacy and Speed communicate his Thoughts to a Friend at any Distance.*

The less than ninety pages of this essay, which introduced the term *cryptography* into the English language, can be read as pure entertainment in only a few hours. Possibly, this is what Babbage did. We may even imagine it was the first work on this topic he came across. If true, it provided him with a rich list of references to the classical literature, some historical background, and a classification of different methods of encipherment illustrated by a variety of examples.

The now traditional subdivision of ciphers into two classes: *substitution ciphers* and *transposition ciphers*, is clearly distinguished in Wilkins' exposition. As we have already seen, a cryptographical substitution is simply a transformation which, preserving the positions of the letters in the plaintext, replaces these letters by other cipher letters, figures or special symbols according to a rule or key. In contradis-

The way of secret writing by equal letters, is, either by changing of

1. Their places, or
2. Their powers.

1. By altering of the places;

Either of the { LINES. LETTERS. BOTH.

1. A man may obscure the sense, by perplexing the order of the lines. If they be written, not only from the left hand to the right, but also from the right hand to the left, as in the eastern languages; or from the top to the bottom, and so upward again, as is commonly related to be usual amongst the inhabitants of Taprobana in the South Sea, with those in China and Japan: according to this following example.

e r f d l e e l l t
i e t o o s w i i h
l s u u h h s n t e
p h o t o a v c s p
p a h t t l t r h e
u n t h e l s e t s
s d i e l n g a o t
y s w a b o n s d i
d p e i a t o e c l
e e g e e b m a n e

In the reading of which, if you begin at the first letter towards the right hand, and so downwards, and then upwards again, you may find these words expressed:

The pestilence doth still increase amongst us; we shall not be able to hold out the siege without fresh and speedy supply.

2. A man may obscure the sense of his writing, by transposing each letter, according to some unusual order

Figure 10A. Bishop Wilkins' description of transposition ciphers (1641)

As, suppose the first letter should be at the latter end of the line, the second at the beginning, or the like.

3. The meaning of any written message may be concealed, by altering the order both of the letters and the lines together. As if a man should write each letter in two several lines. thus:

T e o l i r a e l m s f m s e s p l v o w e u t e l
h s u d e s r a l o t a i h d,u p y s r e m s y i d

The souldiers are almost famished; supply us, or we must yield.

This way may be yet further obscured, by placing them in four lines *, and after any discontinuate order. As, suppose that the first letter be in the beginning of the first line, the second in the beginning of the fourth line, the third in the end of the first, the fourth in the end of the fourth, the fifth in the beginning of the second line, the sixth in the beginning of the third, the seventh in the end of the second, the eighth in the end of the third; and so of the rest: as in this example.

W m r p i t a h h s c t e i n p k e
h a t h f o n o i h k f t o e n i l
a n o e r r o e g t t t h m n v r l
e a u o m h t e i n l e n e t t e s

Which in its resolution is this:

We shall make an irruption upon the enemy from the north, at ten of the clock this night.

This way will yet seem more obscure, if each line be severed into such words as may seem barbarous.

All these kinds may be varied unto divers other more intricate transpositions, according as a man's fancy or occasion shall lead him.

* Or as many more as the length of the epistle shall require.

Figure 10B. Bishop Wilkins' description of transposition ciphers (1641)

tinction, a cryptographical transposition is a transformation which, preserving the identity of the plaintext letters, reorders or permutes their positions relatively to the plaintext according to a rule or key. In these basic forms, whether substitution or transposition, the number of letters in the plaintext equals that of the enciphered message. Wilkins, therefore, talks about secret writing by *"equal letters"*, identifying a substitution by *"changing their powers"*, and a transposition by *"changing their places"*. Figure 10 provides a reprint of his explanation of the latter kind.

The plaintexts of Wilkins' examples reflect that 1641, the year of publication, was the time of a civil war in which couriers, carrying dispatches in cipher, attempted to keep up communication with besieged cities. Pepys told in his diary for 4 February 1665 on Charles I's "surrender" to the Scottish army just before the fall of Newark in 1646: 35)

> *"At noon to dinner to my Lord Belasses, where he told us a very handsome passage of the King's sending him his message about holding out the town of Newark, of which he was then governer for the King. This message he sent in a slugg-bullet, being writ in cypher, and wrapped up in lead and swallowed. So the Messenger came to my Lord and told him he had a message from the King but it was yet in his belly; so they did give him some physique, and out it come. This was a month before the King's flying to the Scotts; and therein he told him that at such a day, being the 3rd or 6th of May, he should hear of his being come to the Scotts, and at the just day he did come to the Scotts"*

The inspiration to Wilkins' little book, *"the fruit of many leisure studies"* as he calls it, came from reading a pamphlet, *Nuntius Inanimatus*, commonly ascribed to a bishop Francis Goodwin. This pamphlet made him so interested in the subject area that he collected all such notes which he came across in other studies. This impression of an academic study rather than of a work derived from any practical experience, is further strengthened by the almost conspicuous lack of information on how to break ciphers.

What prompted Babbage to purchase this two-volume edition of collected works, did not have to be this essay on cryptography. It could as well have been the rather extensive abstract of Wilkins' *Essay towards a Real Character, and a Philosophical Language*. This précis which was printed in 1668 by order of the Royal Society of London, also contained *"An Alphabetic Dictionary: wherein all English Words, according to their various Significations, are either referred to their Places in the Philosophical Tables, or explained by such Words as are in those Tables"*. Wrote Babbage in his autobiography

> *"Previously to my entrance at Trinity College, Cambridge, I resided for a time at Totnes, under the guidance of an Oxford tutor, who undertook to superintend my classical studies only. During my residence at this place I accidentally heard, for the first time, of an idea of forming a universal language. I was much fascinated by it, and,*

> *soon after, proceeded to write a kind of grammar, and then to devise a dictionary. Some trace of the former, I think, I still posses: but I was stopped in my idea of making a universal language by the apparent impossibility of arranging signs in any consecutive order, so as to find, as in a dictionary, the meaning of each when wanted. It was only after I had been some time at Cambridge that I became acquainted with the work of Bishop Wilkins on Universal Language".*

Babbage went up to Cambridge in 1810, so he probably acquired Wilkins' collected mathematical and philosophical works sometime during the period 1811-12. His detailed accounts from those first years at Trinity College contain, according to Hyman, many entries for the purchase of books. Buying this edition, it might have amused Babbage to discover from its account of the author's life, written 1708, that Wilkins once was head of Trinity College, although only for a year. Being married to a sister of Oliver Cromwell's whose path to dictatorship began as member of Parliament for Cambridge, Wilkins obtained this, the most lucrative post at Cambridge, in 1659 by appointment of Richard Cromwell who, after his father's death the previous year, had succeeded him as Lord Protector. Consequently, Wilkins was ejected the following year at the restoration of Charles II. However, what may have looked like nepotism, was in fact a well founded decision.

In 1641, at the publication of his cryptographical treatise, Wilkins was situated in London. With a keen interest in natural philosophy he was one of the small group of men in this city who, according to the famous mathematician John Wallis formed the habit, about 1645, of meeting once a week to a free discussion of scientific affairs. 36) As Wallis noted, there was an urgent need of such private gatherings when the academical studies in both Universities, Oxford and Cambridge, were much interrupted by the Civil Wars. These informal meetings, termed *"our Invisible College"* in the letters of the celebrated chemist Robert Boyle, continued to about 1648. At that time several of the members moved to Oxford by appointment of the committee of Parliament for reforming the university. Among these were Wallis, becoming Savilian Professor of Geometry, and Wilkins, taking up the post of Warden of Wadham College. While the meetings continued in London, drawing so many *"eminent and noble persons"* as to be held regularly and with more formality, a new branch, under the inspiring leadership of Wilkins, was established at Wadham turning the college into a rallying-ground of young scholars. This again attracted many brilliant students one of whom, entering Wadham in 1649, was Christopher Wren, the famous architect. 37)

It was these meetings of free scientific discussion, in London and in Oxford, which in 1660 led to the foundation of the Royal Society, receiving its Royal Charter of Incorporation in 1662. Wilkins, who after his ejection from Cambridge had

moved to London, rejoined the Society in that period and became a member of its council In 1668 he was ordained bishop of Chester. He died in 1672, having gained as a scientist the esteemed reputation, to quote from his eulogy, that "*in whatever subject he undertook, ... he always made* [it] *easier for those that came after him*".

What fascinated Babbage about Wilkins' essay on a *real character* must have been what Clark Emery, in a brilliant analysis [33]) from 1947-48, explained as Wilkins' "*belief that a* [universal] *language to be characterized by facility and usefulness must be founded upon a logical system of classification. What Wilkins proposes to do with words is precisely what Linnæus was later to do with plants*".

The idea that man's vocabulary of words may be organized according to meaning by some taxonomy, beginning with a limited set of the broadest and most inclusive categories and ending with the narrowest, goes back to Descartes and Bacon. Thus the latter remarked upon the virtues of *a real character* that it would represent "*neither letters nor words, but things and notions*" and "*serve for an antidote against the curse of the confusion of tongues*". Here, the classical term of a "real character" implied a concept of notation, understood across the language barriers somewhat in the sense of the positional number system. Wrote Robert Boyle in a letter of 1647:

> "*If the design of the Real Character take effect, it will in good part make amends to mankind for what their pride lost them at the tower of Babel. And truly, since our arithmetical characters are understood by all the nations of Europe the same way I conceive no impossibility, that opposes the doing that in words, that we see already done in numbers*".

Hooke, Wallis, Boyle, Wren, and many other of Wilkins' friends and colleagues helped Wilkins to work out the classifications. Samuel Pepys, the organizer of the British Navy, wrote in his diary for 4 June 1666: "*Thence back with Mr. Hooke to my house and there lent some of my tables of naval matters, the names of rigging and the timbers about a ship, in order to Dr. Wilkins' book coming out about the Universal Language*".

By way of notation Wilkins developed a scheme, assigning consonants or vowels to the different categories, subcategories, etc., so that, down to any level of nesting, the designation was pronounceable as an identifying new "word" conceived as a noun. From this basis, introducing various simple rules, he derived plurals, adjectives, adverbs, and other grammatical forms, until he arrived at what he considered a practical language

In a historical sense the impact of Wilkins work was primarily indirect. It provided a new idea for organization of content matter and purification of prose which, adopted by the eighteenth century members of Royal Society, has made a lasting imprint on English scientific writing

There can be little doubt that Babbage found in this essay a kindred spirit. It definitely broadened his ideas beyond algebra on the importance of notation. Wilkins was among the first to create a scientific notion of data exceeding that of numbers we can add or multiply. Somewhere, in the back of his mind, the impression of Wilkins' universal language must still have been felt, when Babbage much later attempted to assign algorithms for his analytical engine. Of cryptographical importance was the insight it gave Babbage into the structure of language. But it is also interesting to note that the splendid organization of content matter, which is perhaps the most conspicuous trait of Wilkins' cryptographical treatise from 1641, found its way into his classification scheme of the real character. Thus, in the précis, published in the collected works in 1708, it is said: [34])

> "*In the fourth section, he gives us an account of the hieroglyphics of the ancients, which was a mere shift they were put to for want of letters, and was a slight and imperfect invention, suitable to those first and ruder ages. He treats also of the secret and occult ways of writing, taught by the abbot Trithemius, for which he was falsely accused of magic. He gives us some hints about letters or marks used by the ancients for brevity sake; of which nature is shorthand, so common in England.*"

Did Babbage purchase the 1802 edition of Wilkins' works because of his interest in the universal language or in cryptography? We do not know. All we can substantiate, is the fact that his scientific library contained only two works on cryptography In view of the time, effort, and money spent by Babbage to acquire this collection, it seems reasonable to believe that cryptography was not included among his more serious interests.

1.6 APL Terminal Session

Judged by appearance rather than content Babbage's cryptographical papers in the British Library fall into four categories: Letters, notes, newspaper cuttings, and worksheets. So far, we have based our story on facts derived from the former two kinds. The third kind, the cuttings, are predominantly personal advertisements in alphabetic or numerical ciphers. Although hunting primarily for ciphers in the so-called *agony columns*, Babbage also saved a few in plaintext which he found curious, for example because they advertised ciphers for sale.

The number of enciphered advertisements totals about fifteen. If they are organized according to dates of appearance a pattern emerges. Apart from a stray incident from 1845, the all come from the decade 1853-1864. Further, more than half are collected within a period of about one year, from 23. August 1853 to 21. September 1854. Since all of them appeared to have been published in the Times,

I compared the number in Babbage's sample with that of the enciphered advertisements actually published during this decade.[39] Usually located within a small space in the same position, top of second column, on the front page, it was quite easy to ascertain that Babbage had collected only a small fraction. For example, in the period July 31st – December 15th, 1854, there was published twelve enciphered messages, one at a time. Yet in Babbage's sample we find only two of these, namely those from July 31st and September 21st.[40]

This observation should also be compared with Babbage's habits prior to 1853. Although his worksheets contain several solutions of various ciphers, we find instead of cuttings merely handwritten references to newspapers and dates.

To illustrate, in the period 13 September 1833 to 13. September 1835 he was reading a correspondence of no less than sixteen letters which, published variously in the Observer and the Morning Chronicle, were all enciphered in the same monoalphabetic substitution cipher.[41] However, he only kept his translations, so that to procure the originals in cipher one has to trace them using his references. Presumably, he became so proficient reading this cipher that he immediately recognized that "*29 26 26.11.28*" was "*V.D D.K.F.*", being an abbreviation for "*very dear dear kind friend*", while "*15*"was "*M*" for "*Mary*" and "*31*"was "*W*" for "*William*". Guessing abbreviations of this nature, Babbage could rely on a venerable tradition in English letter writing. For instance, in *Journal to Stella*, a series of letters written 1710-1713 by Jonathan Swift, the famous author of *Gulliver's Travels*, we find "*MD*" for "*my dear*", "*ME*" for "*Madam Elderly*" and, appropriate for a master of satire and ambiguity, "*FW*" for "*farewell*" or "*foolish wenches*".

Perhaps the most astounding fact was established investigating the ciphers of Babbage's cuttings. Because here I found that they were carefully selected illustrations of a variety of kinds of ciphers with no type represented by more than at most two applications. In the light of the fact that, in his letter to Mrs. Green (see figure 8B), Babbage told her that he planned to use her research on the cipher of Charles I as illustrations in his book, this seems to suggest only one thing. Namely, that in 1853 Babbage got the bright idea to illustrate his exposition in the *Philosophy of Decyphering* by real-life examples, taken from the agony columns. Further, the fact that he attempted to collect two of each kind, has the obvious interpretation that he intended to use one as illustration of how to break this type of cipher, while the other was meant as an exercise for the reader.

In the following we shall emulate this proposal, substituting Babbage's mechanical aids by an APL-terminal.[42] Indeed, as I see Babbage's cryptographical worksheets, incomprehensible as they may appear, they are nevertheless his log or journal on which he recorded the computational experiments in his cryptographical laboratory. With the APL-terminal as our exploratory tool or cryptographical

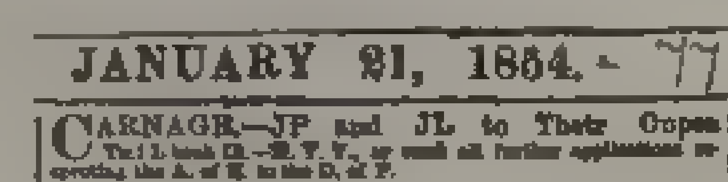
laboratory we can simulate his approach, using terminal sessions as our log to document interactively the computer inputs and outputs. Clearly, this will permit the experiments to be repeated, or validated, by anyone who has access to an APL-terminal.

A fascinating aspect here is the design of a *cryptographic tool-box* of user-defined APL-functions. This can be done in various ways, and the possibilities of inventing new tools are almost unlimited. My proposal for a basis of some thirty functions are documented either in the figures (a few) or in the course of the three terminal sessions, as they are needed. By way of notation, function names are the only identifiers which appear *underscored*. The use of each function appearing in the sessions, is explained in an associated character matrix of the same name but preceded by the double letter: "*CC*".

I see APL as an operational mathematical notation which may be communicated to man and machine.[43] Hence my sole guideline, designing these functions, has been to make them as meaningful as possible in this sense. Valuable inspiration in this respect has been derived from the use of *idioms*[44] and attempts, like that of K. E. Iverson[45], to use APL in expositions of algebra.

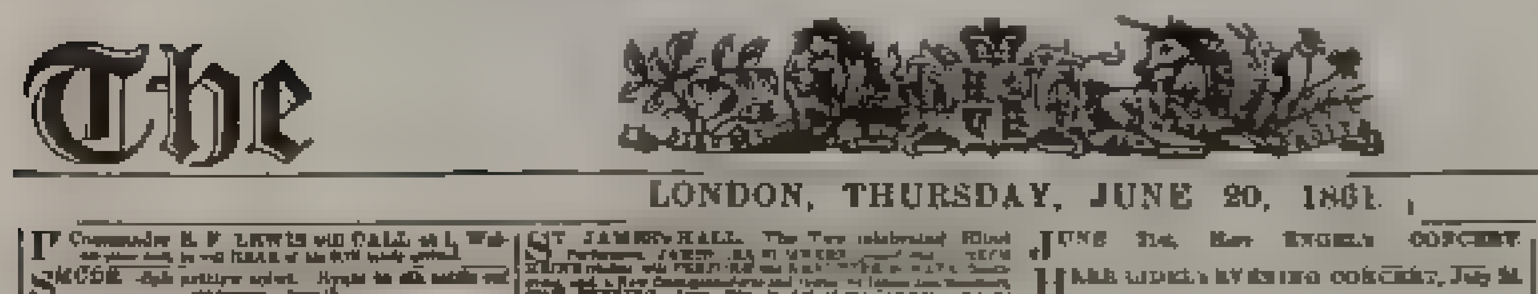
Apart from these more general comments I would like to add the specific one that, although genuinely used in practice, the ciphers we shall now deal with would undoubtedly be considered "appetizers" by Babbage. Nevertheless, the techniques used to break them, are in several cases of fundamental interest.

```
⍝        * * * FALSE WORD DIVISIONS * * *

⍝ INTRODUCING FALSE DIVISIONS OF THE WORDS IN A
⍝ MESSAGE, CREATES A RATHER NAIVE TYPE OF PUZZLE
⍝ YET, CONCEIVED AS A CRYPTOGRAPHICAL TECHNIQUE,
  IT MUST BE CLASSIFIED AS A TRANSPOSITION SINCE
⍝ THE POSITIONS OF THE PLAINTEXT LETTERS ARE
⍝ PERMUTED

⍝ A NEWSPAPER CLIPPING FROM JANUARY 21, 1854,
⍝ FOUND AMONG BABBAGE'S MANUSCRIPTS, DEMONSTRATES
⍝ THE APPROACH (BL. ADD MSS 37205, F 77)
```

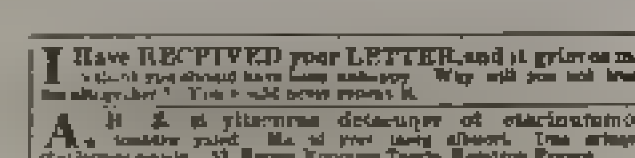

JANUARY 21, 1854. — 77

CARNAGR—JP and JL to Their Copes

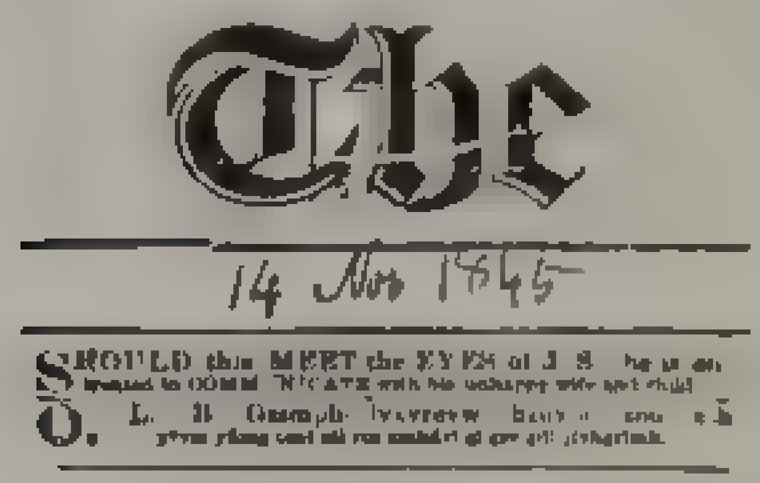
```
⍝          * * * WORD REVERSALS * * *

⍝   HARACTER INPJ

⍝ TO ENTER THIS CRYPTOGRAM INTO THE COMPUTER, LET
⍝ JS DEFINE A CHARACTER INPUT UTILITY FUNCTION
∇ TXTPUT[⎕] ∇
  ∇ M←
[1]  INIT M← 0 0 ⍴
[2]   →ENTER
[3]
[4]
[5]  ENTER →(0≠⍴L←,⍞)/NXT
  ∇
⍝ THE USE OF WHICH MAY BE DESCRIBED

INPUT OF LINES OF VARYING WIDTH, ONE-LINE-AT-A-TIME,
ESTABLISHES A CHARACTER MATRIX  M  WITH A NUMBER OF
ROWS DEFINED BY THE NUMBER OF LINES AND WITH THE
MAXIMUM LINE WIDTH SPECIFYING THE NUMBER OF COLUMNS
          BRANCH OUT BY A CARRIER RETURN! -

⍝

⍝ DECIPHERING THE INTERESTING SENTENCE

THETR OJP A THI L TONH ILL

⍝ WE FIND

HETRI IPEATMILTONHILL
⍝ WHICH, BASED ON THE INDICES OF THE LAST LETTER
⍝ IN EACH WORD  MAY BE RESPACED
I←3 9 11 17

THE TROUPE AT MILTON HILL


⍝          * * * WORD REVERSALS * * *

⍝ THE BACKWARDS SPELLING OF WORDS IS A CLASSICAL
⍝ SCHOOLBOY PRANK. IN A CRYPTOGRAPHICAL SENSE IT
⍝ APPEARS AS A TRANSPOSITION, SINCE IT IS BASED
⍝ ON A REVERSAL OF THE POSITIONS OF THE PLAINTEXT
⍝ LETTERS IN EACH WORD. BY VIRTUE OF THE FACT
⍝ THAT A REVERSAL IS ITS OWN INVERSE ENCIPHERMENT
⍝ AND DECIPHERMENT PROCEED ALIKE

⍝ AN ADVERTISEMENT FROM JUNE 20, 1861, FILED BY
⍝ BABBAGE, DEPICTS THIS (BL, ADD MSS 37205 F 222)
```




```
⍝          * * * WORD REVERSALS * * *

⍝ SOLUTION

⍝ REMOVING ALL PUNCTUATIONS AND THE CONCLUDING
⍝ DATE IN PLAINTEXT THE CRYPTOGRAM MAY BE ENTERED
⍴CRPT222←TXTPUT
SMUDE SAH NETTIRW ECIWT SYATS TA SIH ECIFFO ROF
        EHT TNESERP

2 47

⍝ TO DECIPHER THIS MESSAGE A USER DEFINED
⍝ FUNCTION,  REVERSE , MAY BE INVOKED
⍴⎕←REVERSE CRPT222
EDUMS HAS WRITTEN TWICE STAYS AT HIS OFFICE FOR
        THE                             PRESENT
2 47

⍝ PERFORMING THE REVERSAL

⍝ THE FUNCTION  REVERSE , DESRIBED IN THE
⍝ VARIABLE  CCREVERSE , IS DEFINED AS FOLLOWS

CCREVERSE
RESULT  R  IS THE CHARACTER VECTOR OR MATRIX
 TXT  WITH THE LETTERS OF EACH WORD REVERSED

∇ REVERSE[⎕] ∇
  ∇ R←REVERSE TXT
[1]
[2]
[3]
  ∇

⍝ HERE, TWO THINGS MAY BE OF GENERAL INTEREST

⍝ FIRST, THE TERM  (' '≠TXT)>¯1↓0,' '≠,TXT  IN
⍝ [2] ESTABLISHES A BOOLEAN VECTOR WHICH BY ITS
⍝ 1'S IDENTIFIES A SEQUENCE OF FIELDS, EACH MADE
⍝ UP OF A WORD FOLLOWED BY THE SPACE(S) UNTIL
⍝ THE NEXT WORD

⍝ SECONDLY, THE EXPRESSION  (,TXT)[⌽⌽+\P]  IN THE
⍝ RIGHT HAND PART OF [3] PERFORMS A REVERSAL OF
⍝ ALL THE ELEMENTS IN EACH SUCH FIELD

⍝ A HEART BREAKING MESSAGE

⍝ ANOTHER OF BABBAGE'S CLIPPINGS ILLUSTRATING THE
⍝ SAME IDEA, IS THIS (BL, ADD MSS 37205, F 223)

A B Z SI YLTSENRAE DETSEUQER OT ETACINUMMOC TOUHTIW
YALED MA NI YREV TAERG ELBUORT DNA ERIUQER ETAIDEMMI
ECIVDA - 53 REPPU RUOHYES TEERTS NAMTROP ERAUQS
3 52
```



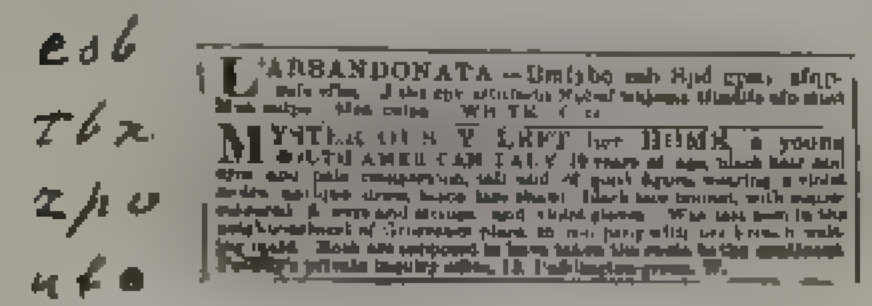
```
⍝          * * * REVERSED ALPHABET * * *

⍝ REPLACING THE LETTERS OF A NORMAL ALPHABET WITH
⍝ THOSE OF A PERMUTED ALPHABET, A REVERSED SAY,
⍝ ESTABLISHES A SIMPLE CIPHER CHARACTERIZED BY
⍝ THE FACT THAT IT PRESERVES THE LETTER POSITIONS
⍝ OF THE PLAINTEXT. THIS TECHNIQUE IS KNOWN AS A
⍝ MONOALPHABETIC SUBSTITUTION BY VIRTUE OF THE
⍝ FACT THAT THE KEY IS THE PERMUTED ALPHABET.

⍝ AN ILLUSTRATION, BASED ON A REVERSED ALPHABET
⍝ AND FOUND AMONG BABBAGE'S MANUSCRIPTS, IS AN
⍝ ADVERTISEMENT FROM THE TIMES, 14 NOVEMBER 1845.
⍝ (BL, ADD MSS 37205, F 42)
```




```
      ⍝ WHICH CRYPTOGRAM IS ENTERED
      ρCRPT42←TEXTPUT
O.L.B.—GSZMPH—IVXVREVW HZUVOB—ZOO SZH
YVVM YFIMG OMT ZTL RM ZMHDVI OL GSV GDL JFVHGRLMH

2 49

      ⍝ NOW, LETTING  ABC  DEFINE THE NORMAL ALPHABET
      ρABC←'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
26
      ⍝ THE CIPHER ALPHABET  XYZ  IS DERIVED
      ρ⎕←XYZ←⌽ABC
ZYXWVUTSRQPONMLKJIHGFEDCBA
26

      ⍝ BASED ON THESE ALPHABETS, TAKING INTO ACCOUNT
      ⍝ THE SPACE AND THE PUNCTUATION MARKS, THE
      ⍝ DECIPHERMENT PROCEEDS AS FOLLOWS
      ρ⎕←(ρCRPT42)ρ(ABC,'—, ')[(XYZ,'—, ')⍳,CRPT42]
J.O.Y.—THANKS—RECEIVED SAFELY ALL HAS
BEEN BURNT LONG AGO IN ANSWER TO THE TWO QUESTIONS
2 49
```



```
⍝          * * * CAESAR ALPHABET * * *

⍝ A CLASSICAL CIPHER, IMPLEMENTING THE TECHNIQUE
⍝ OF MONOALPHABETIC SUBSTITUTION, IS BASED ON A
⍝ CIPHER ALPHABET DERIVED BY A CYCLIC SHIFT OR
⍝ ROTATION OF THE NORMAL ALPHABET TO A NEW POINT
⍝ OF BEGINNING. USED BY JULIUS CAESAR, AMONG
⍝ OTHERS IN ANCIENT ROME, SUCH A ROTATED ALPHABET
⍝ IS KNOWN TODAY AS A 'CAESAR ALPHABET'

⍝ L'ABBANDONATA

⍝ AN ADVERTISEMENT IN THIS CIPHER, CONCERNING THE
⍝ 'ABANDONING' OF SOMEONE, WAS INSERTED ON JUNE
⍝ 23, 1864, BY A PERSON CONFESSING HIS OR HERS
⍝ 'SIN  IN THOUGHTS AND IN WORDS'. SOLVED BY
⍝ BABBAGE IT APPEARS IN HIS MANUSCRIPTS AS
⍝ FOLLOWS (BL, ADD MSS 37205, F 224)
```




```
      ⍝ WHICH MAY BE ENTERED
      ρCRPT224←TEXTPUT
L'ABBANDONATA
— BMFYBO ESB $PDIGPSU SFOPSUFE EFBE.
I TBX ZPV ZFTUFSEBZ
NPSUF WBJOHZ TFBSDIFE UFO XFFLT
MEA CULPA! MEA CULPA! WRITE. — G G.

5 36

      ⍝ TWO REPRESENTATIONS

⍝ A CHARACTERISTIC PROPERTY OF THIS CRYPTOGRAM
⍝ APART FROM THE FACT THAT IT MIXES PLAINTEXT AND
⍝ ENCIPHERED TEXT, DERIVES FROM ITS SOCALLED
⍝ INFORMAL REPRESENTATION  THAT IS, IT PRESERVES
⍝ PUNCTUATIONS AND WORD DIVISIONS

⍝ THE INHERENT WEAKNESS OF THIS REPRESENTATION,
⍝ OFTEN EXPLOITED BY BABBAGE, IS THAT IT PROVIDES
⍝ IMPORTANT CLUES AS TO PROBABLE WORDS, ENDINGS
⍝ ETC.  STILL, TURNING FROM VISUAL INSPECTION TO
⍝ OTHER, MORE COMPUTERIZED APPROACHES, IT MAY BE
⍝ ADVANTAGEOUS TO BRING THE CRYPTOGRAM INTO THE
⍝ FORMAL REPRESENTATION OF A STRING OF LETTERS
⍝ WITH NO SPACING OR PUNCTUATIONS (USUALLY COMMU-
⍝ NICATED IN FIVE-LETTER GROUPS).

⍝ TO ACCOMPLISH A FREE INTERCHANGE BETWEEN THESE
⍝ TWO REPRESENTATIONS, LET US DEFINE A SMALL SET
⍝ OF APPROPRIATE UTILITY FUNCTIONS.
```

```
⍝        * * * CAESAR ALPHABET * * *

      ⍝ IN BOOLEAN FORM

      ⍝ PERHAPS, A BOOLEAN ARRAY IS THE MOST CONVENIENT
      ⍝ FORM IN WHICH THE PECULIAR CHARACTERISTIC OF AN
      ⍝ INFORMAL REPRESENTATION, MAY BE SPECIFIED. A
      ⍝ SUITABLE FUNCTION  THEREFORE, MAY BE THIS
      ∇ PUNCTUATION[⎕] ∇
    ∇ L←PUNCTUATION M
[1]   SYMBOLS L←'           '?
[2]   L←L∘.≠ M
    ∇
      ⍝ WHICH MAY BE EXPLAINED
      CCPUNCTUATION
RIGHT ARGUMENT  M , TRANSFORMED INTO A VECTOR  ,M , IS
SEARCHED FOR THE CHARACTER  SYMBOLS  DEFINED LOCALLY
RESULT  L  IS A BOOLEAN MATRIX INDICATING BY  0  S IN
ROW  I  THE POSITIONS IN ",M  OF THE  I TH SYMBOL.

      ⍝ THUS, CONSIDERING THE MIXED CRYPTOGRAM
      ρL←PUNCTUATION CRPT224
9 180
      ⍝ WE SEE THAT, IN THE PRESENT IMPLEMENTATION, A
      ⍝ SEARCH FOR 9 SYMBOLS INCLUDING THE SPACE, IS
      ⍝ PERFORMED

      ⍝ INVERSE TRANSFORMATIONS

      ⍝ BASICALLY, THE PAIR OF INVERSE TRANSFORMATIONS
      ⍝ BETWEEN THE INFORMAL AND FORMAL REPRESENTATIONS
      ⍝ IS CONCERNED WITH THE QUESTION OF REMOVING OR
      ⍝ RESTORING THE SPECIAL PROPERTY ISOLATED IN THE
      ⍝ LOGICAL MATRIX  L

      ⍝ IN PARTICULAR, TO REMOVE THIS PROPERTY WE MAY
      ⍝ DEFINE A SIMPLE FUNCTION
      ∇ REMOVE[⎕] ∇
    ∇ V←L REMOVE M
[1]   V←(∧⌿L)/,M
    ∇
      ⍝ WHICH MAY BE DESCRIBED
      CCREMOVE
RESULT  V  IS THE VECTOR  ,M , DERIVED FROM THE RIGHT
ARGUMENT  M  BY REMOVAL OF ALL  SYMBOLS . THE LATTER
ARE DEFINED LOCALLY IN THE FUNCTION   PUNCTUATION ,
THE EXPLICIT RESULT OF WHICH FORMS LEFT ARGUMENT  L

      ⍝ TO ILLUSTRATE, THE MIXED CRYPTOGRAM IS BROUGHT
      ⍝ INTO A FORMAL REPRESENTATION AS FOLLOWS
      ρ⎕←AUX←L REMOVE CRPT224
LABBANDONATABMFYDDESBSPDIGPSUSF@PSUFEEFBEJTBXZPVZFTUFSE
      BZNPBUFWDJOMZTFBSDIFEUFOXFBSTMEACULPAMEACULPAWRIT
      EGD
107
      ⍝ CONVERSELY, TO RESTORE THIS PROPERTY WE MAY USE
      ⍝ THE APL IDIOM, APPLIED TO SOLVE THE PROBLEM OF
      ⍝ THE  FALSE WORD DIVISIONS . THIS IS DONE IN
      ⍝ STATEMENT [4] OF THE FOLLOWING FUNCTION
```



```
⍝        * * * CAESAR ALPHABET * * *

      ∇ RESTORE[⎕] ∇
    ∇ W←L RESTORE V,S,⎕IO
[1]   ORIGIN ⎕IO←1
[2]   SYMBOLS S←'        ,   '?
[3]   MAIN W←(⍳ρS)+.×~L
[4]    W←,V S[(W≠0) W]][⍋⍋W≠0]
    ∇
      ⍝ THAT MAY BE EXPLAINED
      CCRESTORE
RESULT  W  IS THE RIGHT ARGUMENT VECTOR  V  EXPANDED
BY  SYMBOLS  FROM THE LOCALLY DEFINED LIST  S , LEFT
ARGUMENT  L  IS A BOOLEAN MATRIX CONTROLLING THIS
OPERATION. ASSUMING THE SYMBOL LIST 'S' TO AGREE WITH
THAT DEFINED IN FUNCTION   PUNCTUATION , THEN "L" IS
THE RESULT OF THAT FUNCTION, WHILE 'V' IS THE RESULT
OF FUNCTION   REMOVE  OR ISOMORPHIC TO THAT RESULT.

      ⍝ NOTE, THOUGH, THAT NO RESHAPING IS PERFORMED.

      ⍝ RUNNING DOWN THE ALPHABET

      ⍝ TO DETERMINE THE NUMBER OF POSITIONS THAT THE
      ⍝ ALPHABET
      ρ⎕←ABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ
26
      ⍝ IS SHIFTED. LET US USE THE FUNCTION  SHIFT' TO
      ⍝  RUN DOWN THE ALPHABET  A SUITABLE SEGMENT OF
      ⍝ THE ENCIPHERED TEXT, QUOTED IN THE FIRST LINE
      ρ⎕←ABC SHIFT 29↑12↓AUX
BMFYBOESBSPDIGPSUSFQPSUFEEFBE
CNGZCPFTCTQEJHQTVTGRQTVGFFGCF
DOHADQGUDURFKIRUWUHSRUWHGGHDG
EPIBERHVEVSGLJSVXVITSVXIHHIEH
FQJCFSIWFWTHMKTWYWJUTWYJIIJFI
GRKDGTJXGXUINLUXZXKVUXZKJJKGJ
HSLEHUKYHYVJOMVYAYLWVYALKKLHK
ITMFIVLZIZWKPNWZBZMXWZBMLLMIL
JUNGJWMAJAXLQOXACANYXACNMMNJM
KVOHKXNBKBYMRPYBDBOZYBDONNOKN
LWPILYOCLCZNSQZCECPAZCEPOOPLO
MXQJMZPDMDAOTRADFDQBADFQPPQMP
NYRKNAQENEBPUSBEGERCBEGRQQRNQ
OZSLOBRFOFCQVTCFHFSDCFHSRRSOR
PATMPCSGPGDRWUDGIGTEDGITSSTPS
QBUNQDTHQHESXVEHJHUFEHJUTTUQT
RCVOREUIRIFTYWFIKIVGFIKVUUVRU
SDWPSFVJSJGUZXGJLJWHGJLWVVWSV
TEXQTGWKTKHVAYHKMKXIHKMXWWXTW
UFYRUHXLULIWBZILNLYJILNYXXYUX
VGZSVIYMVMJXCAJMOMZKJMOZYYZVY
WHATWJZNWNKYDBKNPNALKNPAZZAWZ
XIBUXKAOXOLZECLOQOBMLOQBAABXA
YJCVYLBPYPMAFDMPRPCNMPRCBBCYB
ZKDWZMCQZQNBGENQSQDONQSDCCDZC
ALEXANDRAROCHFORTREPORTEDDEAD
26 29
```

```
⍝       * * * CAESAR ALPHABET * * *

      ⍝ BY WAY OF TERMINOLOGY EACH LINE OF THIS OUTPUT
      ⍝ TABLE IS KNOWN AS A GENERATRIX SINCE IT HAS THE
      ⍝ POTENTIAL FOR GENERATING THE CRYPTOGRAM

      ⍝ CIPHER ALPHABET

      ⍝ THUS, LIKE THAT USED BY THE ROMAN EMPEROR
      ⍝ AUGUSTUS, THE CIPHER ALPHABET  XYZ  DERIVES
      ⍝ FROM A SHIFT OF ONE POSITION OF THE NORMAL
      ⍝ ALPHABET  ABC  TO LETTER  B  AS INITIAL LETTER
      ⍴⎕←XYZ←1⌽ABC
BCDEFGHIJKLMNOPQRSTUVWXYZA
26

      ⍝ THE FUNCTION  SHIFT

      ⍝ AS WILL APPEAR FROM ABOVE THE USE OF THE
      ⍝ FUNCTION  SHIFT  MAY BE SPECIFIED
      DESHIFT
A CHARACTER VECTOR  TXT  IS SHIFTED DOWN THE ALPHABET
 ABC  TO COMPLETE ITS TABLE  T  OF GENERATRICES

      ⍝ CONSIDERING THE OUTPUT FROM THIS FUNCTION IT IS
      ⍝ SEEN THAT, ESSENTIALLY, IT WORKS AS A SET OF
      ⍝ SLIDING ALPHABETS WHICH ARE SHIFTED RELATIVELY
      ⍝ TO EACH OTHER TO SHOW, IN ONE LINE (THE UPPER)
      ⍝ ACROSS THE ALPHABETS, THE STRING OF  TXT

      ⍝ THE FUNCTION MAY THEREFORE BE IMPLEMENTED
      ∇ SHIFT[⎕] ∇
    ∇ T←ABC SHIFT TXT
[1]   T←⍉((ABC⍳,TXT)-⎕IO)⌽((⍴,TXT),⍴ABC)⍴ABC
    ∇

      ⍝ SOLUTION

      ⍝ TO DECIPHER THE CRYPTOGRAM BASED ON THE RESULTS
      ⍝ FOUND PREVIOUSLY, IS NOW STRAIGHTFORWARD
      ⍴PLAIN←ABC[XYZ ⍳2↓¯3↓AUX]
72
      ⍝ HENCE,  REINTRODUCING THE INITIAL AND FINAL
      ⍝ LINES OF PLAINTEXT, IT MAY BE GIVEN THE INFOR
      ⍝ MAL REPRESENTATION
      (⍴CRPT224)⍴ L RESTORE (12↑AUX) PLAIN,¯23↑AUX
L ABBANDONATA
- ALEXANDRA ROCHFORT REPORTED DEAD
I SAW YOU YESTERDAY
MOATE VAINLY SEARCHED TEN WEARS
MEA CULPA! MEA CULPA! WRITE. - G G
      ⍝ REVEALING A SINGLE ENCIPHERMENT ERROR
```

13. May 1859

R[illegible]—Zkb gr brx frw frph ru zulwh iru ph? Vxfk julhi dqg dgalhub!—Rk! Oryh Oryh.


```
⍝       * * * RECIPROCAL ALPHABET * * *

      ⍝ MORE AGONY

      ⍝ ANOTHER OF BABBAGE S CLIPPINGS ILLUSTRATING THE
      ⍝ SAME PRINCIPLE, YET WITH THREE ENCIPHERMENT
      ⍝ ERRORS, IS THIS (BL, ADD MSS 37205, F 221)
      ⍴⎕←CRPT221
ZKB GR BRX FRW FRPH RU ZULWH IRU PH
VXFK JULHI DQG DGALHUB RK ORYH ORYH
2 36


⍝       * * * RECIPROCAL ALPHABET * * *

      ⍝ AN ILLUSTRATION OF A SIMPLE OR MONOALPHABETIC
      ⍝ SUBSTITUTION BASED ON A RECIPROCAL ALPHABET IS
      ⍝ THE CIPHER IN THE TIMES, 31 JULY 1854.
      ⍴⎕←TMS540731
T H E O
-BIT AI CZYO OYSR OFIVI MLYSTER.-
      UITF, A, DYZIU.
3 33
```

31 July 1854

THEO.—Bit ai czyo oysr ofivi mlyster.—Uitf, a, dyziu.

```
      ⍴L←PUNCTUATION 0 1 1⍴TMS540731
9 66
      ⍴⎕←C31←L REMOVE 0 1 1⍴TMS540731
BITAICZYOOYSROFIVIMLYSTERUITFADYZIU
35
      ⍴⎕←ABC SHIFT ABC[(⍋ABC)⍳C31]
YRGZRXABJLRHITURERNOBMOVIFRGUZWDARF
ZSHASYBCKMCIJUVSFSOPCIHWJGSHVAXCBSG
ATIBTZCDLNDJKVWTGTPQDJIXKHTIWBYDCTH
BUJCUADEMOEKLWXUHURQEKJYLIUJXCZEDUI
CVKDVBEFNPFLMXYVIVRSFLKZMJVKYDAFEVJ
DWLEWCFGOQGMNYZWJWSTGMLANKWLZEBGFWK
EXMFXDGHPRHNOZAXKXTUHNMBOLXMAFCHGXL
FYNGYEHIQSIOPABYLYUVIONCPMYNBGDIHYM
GZOHZFIJRTJPQBCZMZVWJPODQNZOCHEJIZN
HAPIAGJKSUKQRCDANAWXKQPERDAPDIFKJAO
IBQJBHKLTVLRSDEBOBXYLRQFSPBQEJGLKBP
JCRKCILMUWMSTEFCPCYZMSRGTQCRFKHMLCQ
KDSLDJMNVXNTUFGDQDZANTSHURDSGLINMDR
LETMEKNOWYOUVGHEREABOUTIVSETIMJONES
MFUNFLOPXZPVWHIFSFBCPVUJWFUJNKPOFT
NGVOGMPQYAQWXIJGTGCDQWVKXUGVJOLQPGU
OHWPHNQRZBRXYJKHUHDERXWLYVHWKPMRQHV
PIXQIORSACSYZKLIVIEFSYXMZWIXLQNSRIW
QJYRJPSTBDTZALMJWJFGTZYNAXJYMROTSJX
RKZSKQTUCEUABMNKXKGHUAZOBYKZNSPUTKY
SLATLRUVDFVBCNOLYLHIVBAPCZLAOTQVULZ
TMBUMSVWEGWCDOPMZMIJWCBQDAMBPURWVMA
UNCVNTWXFHXDEPQNANJKXDCREBNCQVSXWNB
VODWOUXYGIYEFQROBOKLYEDSFCODRWTYXOC
WPEXPVYZHJZFGRSPCPLMZFETGDPESXUZYPD
XQFYQWZAIKAGHSTQDQMNAGFUHEQFTYVAZQE
26 35
```

```
⍝     * * * RECIPROCAL ALPHABET * * *

      ρL←P↑ABC[(13⌽⍳ABC),C31]
,FTHEKNOWYOJVGHEREABOUTIVSETHMJONES
3F
      (ρTMS540731)ρTMS540731[1 3,L RESTORE P
T H E ,
 LET ME KNOW YOJV GHERE ABOUTIV,-
         SETH, M, JONES

      ⍝ THREE ENCIPHERMENT ERRORS AND ONE MISPRINT.

      ⍝ RECIPROCAL ALPHABET
      ρL←PQR←ABC [0 ⌽1]⌽⍳ABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ
M K IIHDFLJLC BAZYXWVUTSNQFLN
  ,6
      ↑ 2 13ρ( 2 13↑PQR)  2  13↑PQR
ABCDEFGHIJKLM
MLKJIHGFEDCBA

NOPQRSTUVWXYZ
ZYXWVUTSRQPON
```


2.1 The Philosophy of Analysis

Babbage's choice of title: *The Philosophy of Decyphering*, is perhaps the most obvious indication that he planned a scientific treatise. Today we might think this title somewhat pompous. At the time, however, when physics was still "natural philosophy" the connotation was appropriate, particularly as its author held Newton's chair at Cambridge. Yet most significant, seen in retrospect, is the tie between this choice and the most important contribution of his youth: *The Philosophy of Analysis*, a series of mathematical essays written primarily in the years 1818-22.

Except for one and parts of another, these essays were never published. Although presented to the Cambridge Philosophical Society, they were not even finished by Babbage. Pushed aside by the work on his Difference Engine, they did not influence contemporary work in mathematics. Filed in the British Library[1]) after his death, the manuscript was left dormant until John M. Dubbey in 1978 reviewed its contents in his book: *The Mathematical Work of Charles Babbage*,[2]) concluding that *"The mathematical world is poorer through Babbage never having developed nor published the 'Philosophy of Analysis', since ... the work contains some exceptionally fine material with the promise of better to come"*.

According to Dubbey, Babbage states in his introduction: *"It is my intention in the following pages to attempt an examination of some of those modes by which mathematical discoveries have been made"*. Keywords like notation, induction, generalization, analogy, artifices, and games, all selected from the titles proposed by Babbage, suggest the general attitude of this work. When therefore the mathematician G. Polya claimed in his delightful book *How to Solve It* [3]) from 1944, that he was presenting *"a new aspect of mathematical method"*, he was only partly right. Unknown but to a few intimate friends, Babbage had explored the field more than a century earlier.

Three topics Babbage dealt with specifically in these essays, are of particular relevance to an understanding of his cryptographical work. Creating the necessary foundation for introducing mathematical reasoning into what had been, until then, basically a non-mathematical world, these subjects are: Notation, permanence of form, and *"a new mode of analysis"* then called the geometry of situation. Assigned each an essay by Babbage, they will be treated in order.

Notation was the only topic on which Babbage actually published. This happened when parts of his proposed essay appeared as an article, entitled *Notation (in mathematics)*, in the Edinburgh Encyclopedia in 1830.[4]) For some reason or other the printing was delayed, for Dubbey found among Babbage's papers in the British Library a letter, dated 25 February 1822, in which Sir David Brewster, the editor of the Encyclopedia, wrote: "*I enclose a Proof of your Article on Notation*". Babbage introduced this rather perceptive article by defining its topic as "*the art of adopting arbitrary symbols to the representation of quantities, and the operations to be performed on them*".

The main purpose of the article was to prescribe general rules of notation for those wishing to express newly discovered relationships or to abbreviate those already in use. It is too far from our main theme to discuss these rules, but let me just list them in the order given by Babbage, to give perspective to the debate on notation in programming languages taking place even today

- *All notation should be as simple as the nature of the operations to be indicated will admit.*
- *That we must adhere to one notation for one thing.*
- *Not to multiply the number of mathematical signs without necessity*
- *When it is required to express new relations that are analogous to others for which signs are already contrived, we should employ a notation as nearly allied to those signs as we conveniently can.*
- *Whenever we wish to denote the inverse of any operation, we must use the same characteristic with the index -1*
- *That every equation ought to be capable of indicating a law*
- *It is better to make any expression an apparent function of n, than to let it consist of operations n times repeated*
- *That all notation should be so contrived as to have its parts capable of being employed separately.*
- *All letters that denote quantity should be printed in Italics, but all those which indicate operations, should be printed in Roman Character.*
- *Every functional characteristics affects all symbols which follow it, just as if they constituted one letter*
- *Parentheses may be omitted, if it can be done without introducing ambiguity.*

Some of these rules are not original to Babbage. In his introduction he observes that "*brevity appears to have been the directing principle which guided the early cultivators of the algebraic art*". Evidently, this has a bearing on his third rule which, in a historical light, is but a restatement of *Ockham's Razor*, the dictum propounded in the early 14th century by the Franciscan friar William of Ockham in his criticism

of the "*Five Ways*" or five "proofs of God's existence" by St. Thomas Aquinas Although slightly misquoted, the traditional statement in Latin of this principle is: "*Entia non sunt multiplicanda sine necessitate*", or entities should not be multiplied without necessity.

Somewhat artificially Babbage perceived this synthesis of rules in his article as distinct from the analysis of notational incidences in his first essay: *On the Influence of Signs in Mathematical Reasoning* [5]) Published 1826 Babbage elegantly summed up its contents in the conclusion.

"*I have now enumerated what appear to me to be the principle causes which exert an influence on the success of mathematical reasoning, and have illustrated, with examples, those which were susceptible of it. They may be recapitulated in few words. The nature of the quantities which form the subject of the science, together with the distinctness of its definitions – the power of placing in a prominent light, the particular point on which the reasoning turns – the quantity of meaning condensed into small space – the possibility of separating difficulties, and of combining innumerable cases, – together with the symmetry, which may be made to pervade the reasoning, both in choice, and in the position of the symbols, are the grounds of that pre-eminence, which has invariably been allowed to the accuracy of the conclusions deduced by mathematical reasoning*".

The subject of the principles and the laws of notation was ever present in his mind and, eventually, he came to see his computers, the Difference Engine and the Analytical Engine, as dependent upon notational principles. This interest in notation took form during his undergraduate years at Cambridge University when, together with his two friends John Herschel and George Peacock, he introduced Leibnitz' differential notation to Great Britain. A paper, *Observations on the Notation employed in the Calculus of Functions*, [6]) published in 1820, contains a suggestion of some appeal to a modern computer scientist. Namely, for the sake of facility in printing, to give up the use of superscript or subscript indices and instead "*bringing the indices down to the level of the functional sign and inclosing them between two bars*".

2.2 The Principle of Permanence of Form

The principle of the permanence of equivalent forms or, as it is often abbreviated, the principle of permanence, is a heuristic guideline. Related to Babbage's fourth rule on the use of identical or similar notation for analogous relationships, it prescribes that the validity of calculating or arithmetical laws should be retained, as their forms are generalized to algebraic laws extending the concepts of the mathematical objects connected by them.

The classical example, quoted since the days of what has been dubbed "The Cambridge Network": the mathematical clique of Babbage and his friends, related

to a simple arithmetical law. Powers with the same basis are multiplied by raising the basis to the power given by the sum of the exponents, or $a^m \times a^n = a^{m+n}$. Since a^n, the nth power of a, is merely a shorthand notation for a multiplied by itselves n times this calculating law evidently derives from experience. Invoking the principle of permanence the form of the law is generalized to an algebraic statement holding without exception for all integers. One has now to account, therefore, for the case a^{m-n} where $m=n$ or $m<n$ are wholly without meaning in relation to the original definition of the nth power of a. The way out according to the principle of permanence, is to extend the concept of the mathematical object a^n introducing, as is well known, the definitions: $a^0=1$ and $a^{-n}=1/a^n$ for all $a \neq 0$.

In Babbage's encyclopedic article on notation, this example identifies his fourth rule as a statement of the principle of permanence: [4]

> *"That analogy ought to be our guide in the formation of all new notations, is a truth, which, like many others, has been felt and acted upon, although it may not have been stated in express terms: and it was probably this feeling which induced Stifelius to inquire into the meaning of negative exponents, the consequence of which was the establishment of the connection between the direct and reciprocal powers, a deduction which, when enlarged by the consideration of fractional exponents, was no mean addition to the state of algebra at the time it was suggested".*

To have the reader appreciate the import of this statement, Babbage implicitly refers to the thorough historical account given in his introduction. Here we are told that "*Stifelius* [Michael Stifel[7]], *a German, who published a work, entitled Arithmetica Integra, Norimburg, 1544, added considerably to the use of signs*". Further, that Bombelli and Simon Stevin made the most valuable innovations towards the present notation of powers; and that the latter not only observed that "*the power, whose index is zero, is equal to unity*", but also that he "*went a step beyond his predecessors, and denoted roots by fractional indices*". A casual reference in Babbage's description: "*according to Dr. Hutton*", suggests that his main source on these historical facts was Charles Hutton's *Tracts on Mathematical and Philosophical Subjects*, published in London 1812. Indeed, checking Tucker's catalogue, I found not only that Babbage's library contained this work, but also that the three-volume treatise was a presentation copy with the donor's autograph upon it.

The modern view on this principle, as expressed by mathematicians of today, is rather condemning. For instance, in his inspiring *Mathematics: The Loss of Certainty* from 1980 Morris Kline wrote: [8]

> *"The principle was essentially arbitrary and begged the question of why various types of numbers possess the same properties as the whole numbers ...* [It] *treats algebra as a science of symbols and their laws of combination. This foundation was both vague and*

> *inelastic. Its advocates insisted on a parallelism between arithmetical and general algebra so rigid that, if maintained, it would destroy the generality of algebra, and they never seem to have realized that a formula true with one interpretation of the symbols might not be true for another".*

Although Babbage was vague on this point, it would be seen that, in the discussion of his sixth rule on every equation indicating a law, he considered this requirement so important that, in case of conflict, analogy or permanence of form had to yield.

> *"Analogy to those* [signs] *which form the established language of the science, although of great importance, cannot be admitted to supersede the rigid enforcement of that we are now considering: happily however, the two principles will rarely be found at variance, for those symbols, and those inflexions of symbols, (if the term may be allowed,) which long experience has naturalized, generally furnish the most correct models of imitation."*

Evidently, Babbage's view on the principle of permanence was far more flexible than the interpretation by Kline. But let us not blame Kline for this somewhat biased picture. Because quite surprisingly, the past few years since the publication of his book has seen a spate of articles [9]) which, based on ongoing historical research into the unpublished source material, has drastically changed the understanding and the perspective of the development of modern algebra in early 19th-century England. The origin and the motivation of this research was a puzzling question of priority.

Until Dubbey published his book in 1978 on Babbage's mathematical work, it was considered an established historical fact that the enunciation of the principle as well as its name, were the contributions of Babbage's friend, George Peacock, in his *A Treatise on Algebra* from 1830. That the same year also saw Babbage's publication of the principle, in his article on notation written 1821-22, went unnoticed. Contrariwise I have found, as a curiosity, that in German literature [10]) it has been ascribed to Herman Hankel who endorsed it in 1867 in his *Theorie der complexen Zahlensystem*, the work which established Hankel as the creator of a logical theory of rational numbers. However, born in 1839 and author of a couple of authoritative books on the history of mathematics, Hankel himself would undoubtedly have declined this honour.

What Dubbey discovered was that one of Babbage's unpublished essays, entitled "*General notions respecting Analysis (my theory of identity)*", was almost identical in argumentation and formulation – apart from choice of name – to Peacock's presentation of the principle. Further, from their correspondence in the British Library he established that in 1822 Peacock had "*read the greater part of them* [the essays] *over very attentively*". Yet the friendly tone of their letters also after 1830,

reveals that, to quote Dubbey, "*there is not a shred of additional evidence to support a charge of plagiarism or even collusion*".

The astonishing similarity between Babbage's unpublished and Peacock's published work inspired new efforts to examine the historical records. Harvey W Becher most convincingly proposed that Babbage and Peacock extended ideas put forth in 1803 by Robert Woodhouse (1773-1829). From Babbage's *Passages*, we know that at Cambridge "*I now employed all my leisure in studying such mathematical works as accident brought to my knowledge. Amongst these* ... [was] *Woodhouse's 'Principles of Analytical Calculation' from which I learned the* [differential] *notation of Leibnitz*". This book by Woodhouse, professor at Cambridge, was the first work published in England on this topic. It so inspired Babbage and his undergraduate friends that in 1812 they formed the *Analytical Society* to promote the replacement of Newton's fluxions with Leibnitz's calculus. Babbage left Cambridge after graduating in 1814, but he maintained a close association with his Cambridge friends in the Society, creating in their group through discussions and exchange of unpublished works, as Babbage noted in 1817, a "*mania analytica*".

Ostensibly concerned with the problem of notation, they endeavoured to divorce the foundations of "*pure analytics*" from intuitive or physical considerations. To effect their program, they advocated the teaching of the abstract principles of analysis prior to its applications, in preference to the traditional Cambridge method of teaching technique through physical problems of limited scope. As a consequence, their emphasis in algebra shifted from the meaning or interpretation of symbols or signs to the laws of operation. A development, Helena Pycior pointed out, similar in spirit and effect to the introduction into physics during the Scientific Revolution of a concern for the "how" rather than the "why". Thus, in 1816 Edward Ffrench Bromhead, one of the founding members of the Society, wrote Babbage: "*You talk of some very new views on the foundations of analysis. I am on the same subject and have an idea wholly divesting it of any connection with number or quantity, but making it such that it may be applicable to any thing*". On this background it is understandable that neither Babbage nor Peacock were overly concerned with acknowledgements. Their approach to algebra was simply not unique at Cambridge.

The novel idea that the laws of algebra could be assigned rather arbitrarily made it necessary, it was felt, to introduce a principle of selection of the laws. Even if in the finished version, as stated by Peacock, algebra like arithmetic or geometry is a deductive science derived from axioms. Only, the problem was that algebra did not suggest self-evident or empirically necessary axioms, so they had to be derived working backwards from the laws of operation. The permanence of form, carried over from arithmetic, was therefore their choice of a principle of selection. As Becher has documented, this principle originated with Woodhouse who termed it

"*the notions of the extensions of demonstrated forms*". A fact, incidentally, Peacock acknowledged in 1833, saying that Woodhouse made "*a very near approach*" to his own principle.

The novelty of these ideas is perhaps best illustrated by the negative reaction of Sir William Rowan Hamilton to Peacock's *Treatise* of 1830. In the early 1840s, Hamilton said, according to Pycior:

> *When I first read that work ... and indeed for a long time afterwards, it seemed to me, I own ... that the author designed to reduce algebra to a mere system of symbols, and* nothing more; *an affair of pothooks and hangers, of black strokes upon white paper, to be made according to a fixed but arbitrary set of rules: and I refused, in my own mind, to give the high name of* Science *to the results of such a system, as I should, even now, think it a stretch of courtesy, however it may be allowed by custom, to speak of chess as a "Science", though it may well be called a "scientific game"*.

Yet, by his invention in 1843 of a new kind of four-dimensional numbers, the so-called quaternions, Hamilton became the first to exercise this freedom of mathematics in that he had to abolish with the commutative law of multiplication: That a product is independent of the order of its factors. Of course, Hamilton simultaneously destroyed the principle of permanence in its strict interpretation by Peacock and others that algebra was a generalization of all the forms of arithmetic. His discovery confirmed Babbage's vague visualization that conflicts, although rare, could not necessarily be avoided, and that in these cases analogy, in the sense of permanence of form, would have to yield to statements of law. If therefore Babbage, inspired perhaps by Peacock and others, had rejected the possibility of such conflicts in his later but unpublished essay on "*my theory of identity*", Hamilton's contribution made this position untenable. As demonstrated by Boole, Cayley, and Sylvester, to mention a few, the principle of permanence evaporated from the further development of "*pure analytics*" into a modern axiomatic algebra. Nevertheless, the idea of permanence of form remained, but now in the far more abstract sense of so-called *algebraic invariants* completely dissociated from any notion of arithmetical analogies. Starting with a contribution by George Boole in 1841, Cayley was attracted to this work and in turn interested Sylvester in the subject. The term "*invariant*" is due to the latter.

In his exposition of the principle of permanence Peacock saw it exclusively from the viewpoint of generalizing arithmetic into algebra. However, as I understand Dubbey's quotations from Babbage's unpublished essays, Babbage admitted a wider interpretation, placing geometry and physics as additional areas upon which a generalized algebra can draw by analogy:

To the dominion of number which algebra now possessed Descartes added that over space and large as was this addition to its empire it was perhaps scarcely less valuable as pointing out the road to other acquisitions ... The representation of time and force by means of letters and the applications of algebra to mechanics, optics and other parts of natural philosophy follows with little effort when the road was once opened.

Considering the historical development of mechanics, a striking incidence immediately comes to mind. Antedating Babbage's undergraduate years at Cambridge, it appears highly likely that he happened to study this case during his inquiry into the problem of the differential notation. Pertaining to the definition of equilibrium for a mechanical system, it is concerned with the preservation of form under some physical generalization which eventually can be given a geometrical interpretation. The point is that what is true in a physical or geometrical sense, cannot depend upon the arbitrary choice of a reference frame. To bring out this invariance in the algebraic formulation we desire to associate with every law a permanence of form, independent of the reference frame in which it happens to be used. With Descartes, geometry was tied up with algebra. What is found to be a geometrical invariance, must therefore also be possible to express as an algebraic invariance. This is the novel perspective in the notion of permanence of form which, as we shall see later, attempts to break the surface in some of Babbage's work.

From antiquity, the term *equilibrium* has been used to denote the state of rest of a mechanical system. Meaning literally in Latin "equal weight" or "equal balance", the term refers to the condition that the system is *static*. Namely, that the collected forces upon the system outweigh or balance each other. In mathematical terminology, the vectorial sum of the forces is zero.

Careful consideration will show that it is utter nonsense to use this term to describe a dynamic system. An accelerated system is definitely not at rest and, furthermore, the reason it is accelerated, is that the forces do not balance but have a component which, according to Newton's Second Law, accelerates the system. Notwithstanding this, as we all know, physicists, engineers, and even economists of today do not hesitate to talk about the equilibrium of a dynamic system, and with good reason. Because the modern connotation, generalizing the term from static to dynamic systems, has been accomplished invoking the notion of permanence of form to preserve the original condition of the forces, but with a new interpretation containing the old one as a special case.

This generalization is due to the French philosopher and mathematician, Jean Le Rond D'Alembert, who, dissatisfied with some of Newton's work, published his result in 1743 in his *Traité de dynamique*. To explain how bodies (ships, cars, or aeroplanes) move without disintegrating, he formulated his celebrated principle underlying the entire discipline of analytical mechanics. *D'Alembert's principle* simply

says that the *internal* forces of a body in motion satisfy the equilibrium condition of a system at rest. [11]) Actually, using the relative velocities of the individual parts rather than the internal forces in his original formulation, he postulated that these relative velocities (internal forces) had to balance, because otherwise the individual pieces of the body would come apart.

As simple as it was elegant, this intuitively obvious observation paved the way for an entirely new formulation of dynamics. First, one could forget all about the internal forces because they summed to zero anyhow. Secondly, the external forces being much fewer and far better defined, would determine the state of the system. If they had a component (a nonzero sum) the system would accelerate.

The former condition inspired Leonhard Euler, the great Swiss mathematician and dominant theoretical physicist of the 18th century, to a new formulation invoking the idea of permanence of form once more. Considering Newton's Second Law for a body in motion, he simply substituted the term: mass times acceleration by a new artificial force, known today as the *force of inertia*. Subtracting this artificial force from the external forces of the body the vectorial sum had now to balance, giving the term: equilibrium a new and more general interpretation for dynamic systems.

I think that most students of physics will agree that, while it is easy to appreciate d'Alembert's contribution, all there apparently is to Euler's is a mere substitution of one name for another. The point, however, is far more subtle. Euler's contribution is that we can use one and the same equation to formulate the condition of equilibrium for all systems, whether static or dynamic. He unified statics and dynamics from the viewpoint of problem formulation. This is the difficult problem. From there on, a solution can always be found in a routine manner.

Lagrange, in his celebrated *Méchanique analytique* from 1788, used this approach to extend his fundamental principle of virtual work from static to dynamic systems. This book was not only in Babbage's library, but he surely must also have read it in connection with his intensive study of Leibnitz's differential notation. In fact, Babbage referred to the book in his article from 1826. [5]) Further, in his library Babbage had the second edition from 1758 of d'Alembert's treatise on dynamics. We may therefore imagine that Babbage not only observed this application of the permanence of form. We may also assume that he interpreted Euler's contribution as an invariance under a geometrical transformation of space. Namely, that Euler introduced a new reference frame moving in step with the dynamic system, so that observed from this new frame it appeared as if the system was at rest. Thus, in a geometrical perspective the only difference between static and dynamic systems would be the choice of reference system. To reflect this in the algebraic formulation of the equilibrium condition, threw the principle of permanence into a new role.

2.3 A Question of Relative Position

Perhaps most closely related to his cryptographical work, is Babbage's last essay which he called, *"Of problems requiring new methods where the difficulty generally consists in putting it into analytical language"*. A title, which he subsequently changed into: *"Of questions requiring the invention of new modes of analysis"*. After having read it Peacock expresses the opinion, in a letter of 7 May 1822, that it *"will be charming when completed"*. Of course, it was never completed. Further, what little there is, the word "charm" is quite misleading. Rather, the striking impression is one of uncanny insight. Because to catch the vague and intuitive notion of system structure, Babbage attempted to introduce topology or geometry of situation, as it was then called. And this at a time when this discipline had seen almost no development since the early work of Euler.

At the outset of the essay, according to Dubbey, Babbage makes the point that the problems of physics usually result in a neat algebraic formulation which can be solved either directly or by approximation. Alluding to a remark by Leibnitz that *"Few occasions call forth the ingenuity of mankind more than those games which they contrive for the occupation of their leisure"*, Babbage then proposes to deal with some logical problems which normally defy such a mathematical analysis: [12])

> *"The nature of these questions to which we shall now direct our attention is entirely different and for by far the greater part of them all known methods are inefficient. The first great difficulty then presented to us is that of representing in symbolic language the conditions of the problem. Unless this can be accomplished all hope of solution must be given up and an approximation, supposing the question to admit of one, cannot be discovered. The class of questions to which I allude chiefly comprise such as are referable to the Geometry of Situation and have very frequently arisen from games of skill"*.

Geometria situs, or geometry of situation, was an expression introduced by Leibnitz to designate a branch of geometry depending upon relative position rather than upon a metric measure like distance or angle. The first to deal seriously with this topic was Euler who, in a now famous paper on *The Seven Bridges of Königsberg* published in 1735, founded modern graph theory – the theory in which mathematical relationships of precedence (or of equality) are represented geometrically by nodes interconnected by arcs that is (or is not) given an orientation. Gauss, I think, changed the name of the topic area to *analysis situs*, the analysis of (relative) position, and it was one of his students, Johann Listing, who in 1847, in the first systematic treatise in the field: *Vorstudien zur Topologie*, introduced the modern term *topology*. Gustav Robert Kirchhoff's formulation in the previous year of his two celebrated laws of electric network theory, demonstrated in practice the fantastic potential of graph theory as he had extended it by fundamental concepts like trees and meshes. [13])

In a popular sense topology is a rubber geometry, being concerned with those properties that are preserved under distortions. From this point of view, according to a classical joke, there is no difference between a coffee cup and a doughnut, since they both contain a single hole. Indeed, considering the transformation between these two geometrical figures it may be visualized that there is a unique correspondence, point to point, between the two figures, simultaneously as neighbouring points are mapped into neighbouring points. The amazing fact is that mathematicians, from an identification of these two properties, have been able to establish a theoretically advanced geometry of relative position and an associated and very powerful algebra. Still, in the 1820's when Babbage was writing about this topic area, it was all in the future.

As a student at Cambridge University Babbage soon came to see the required mathematical studies as an intellectual trudging over barren lands. Their sole purpose was to pass an examination. Thus, having been discouraged by several of his tutors in his attempts to reach a deeper understanding, Babbage, as he explained in his autobiography, *"acquired a distaste for the routine of the studies of the place, and devoured the papers of Euler and other mathematicians, scattered through innumerable volumes of the academies of Petersburgh, Berlin, and Paris, which the libraries I had recourse to contained"*. Like so many other would-be scientists, Babbage became aware of his higher goal in life by being brought into contact with the original writings of the great masters of the past.

Undoubtedly, it was Euler's fascination of games and puzzles that inspired him. For example, in 1817 he published a paper, entitled *"An Account of Euler's Method of solving a problem, relative to the Move of the Knight at the Game of Chess"*. [14]) The problem referred to, Babbage briefly summarized in the paper by the words: *"The Knight being placed on any given square of the chess-board, it is required at sixtythree successive moves, to cause it to move over the remaining sixtythree squares"*.

In this problem like in most others belonging to the category of party games or tricks, the point of fundamental interest is not distance but the *properties of relative position*. What captivated Babbage's imagination in this respect, was Euler's attempt to invent an algebraic interpretation for reasoning about its solution. This Babbage made perfectly clear in his opening statement: *"To most of those who are familiar with the Game of Chess, this curious question is perhaps well known, although the method of reasoning which Euler employed in discovering its solution, is, I believe, not so generally understood"*. Definitely, it was the challenge of inventing an algebraic interpretation of the problem of relative position, that was implied by the title: *"Of questions requiring the invention of new modes of analysis"* of his unpublished essay.

In his discussion of this essay, Dubbey gives a detailed account of Babbage's analysis of the game of tic-tac-toe or noughts-and-crosses. What is of the interest in the present context is Babbage's observation that on a board of 3-by-3 cells, the strategy leading to a winning position of three crosses (noughts) in a line (row, column, or diagonal from upper left to lower right, or from upper right to lower left), may be expressed in terms of the fundamental properties of *magic square.* [15]

The notion of a magic square dates back some three thousand years to Ancient China. Leonhard Euler was one of several mathematicians who found them amusing and worth studying. They appear to have been of equal interest to the layman. An amusing archeological find illustrating this, is a wooden ruler for navigational computations, salvaged from the Danish-Norwegian frigate "Lossen", which was wrecked by a hurricane near the coast of Norway on Christmas night 1717. On this ruler (see figure 11), a cadet or an officer on one of the long watches had carved a magic square, summing to 15 along every row, diagonal, or column.

6	1	8
7	5	3
2	9	4

Babbage's idea considering squares of this kind, was that an alternative representation of the game would be with the two players A and B alternately selecting numbers between 1 and 9, the object being to find any three which would add up to 15. The power of this reformulation of the game, was that it enabled Babbage to arrive at an algebraic formulation. As Dubbey quotes him saying: "*The plan was proposed rather with a view of showing the possibility of the thing than as being convenient for executing it*".

In general, a magic square is an array of the first n^2 integers arranged in n rows and n columns, so that the sum of the numbers in each row, column, or principal diagonal (upper left to lower right and upper right to lower left) is *magic*. To be specific, each of these sums is equal to $n(n^2+1)/2$. Any square of odd-order n may be constructed according to a simple algorithm which, placing the integers from 1 up to n^2 in the "cells" or positions of the square in consecutive order, may be rendered as follows: [17]

> "*Begin by placing the number 1 in the middle cell of the bottom row; after filling a cell in the bottom row, place the next number in the cell at the top of the next column on the right, as far as possible fill the cells in a downward diagonal line from left to right; upon filling a cell in the last right-hand column of the square, place the next number*

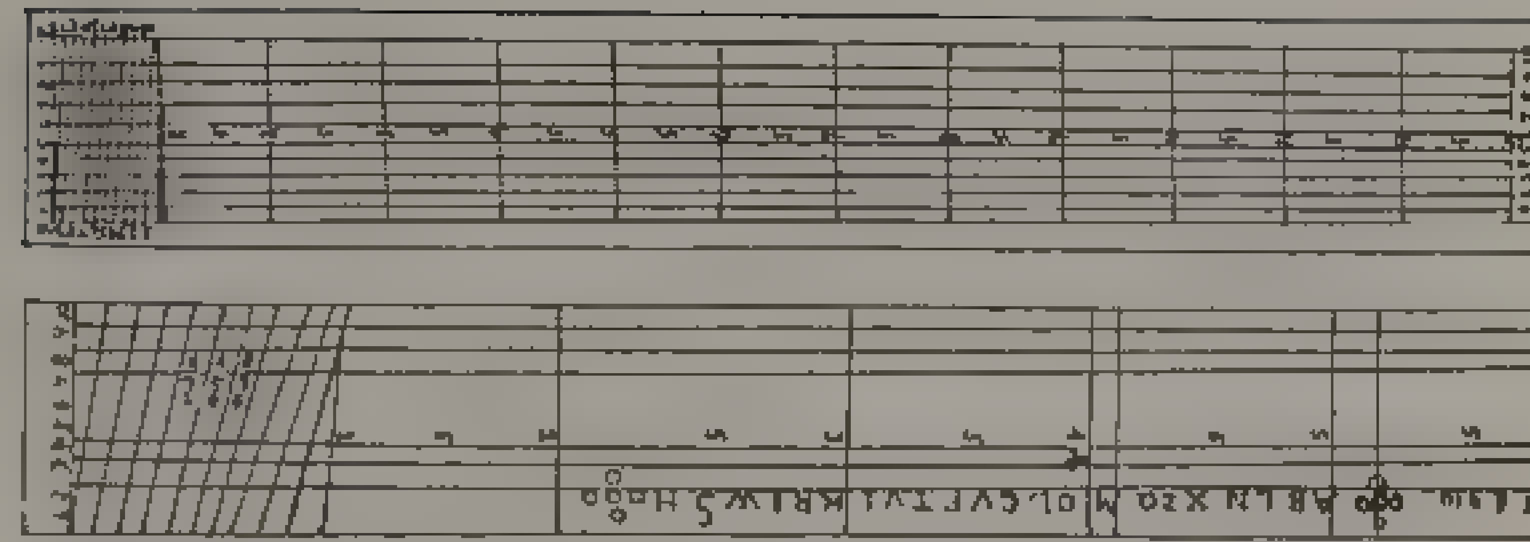


Figure 11. Magic square carved into a navigational ruler [16] Made of fruit-tree the ruler was salvaged from the Danish-Norwegian frigate "Lossen", wrecked off the coast of Norway 1717 (Courtesy Norsk Sjøfartsmuseum).

> *in the cell at the extreme left of the next lower row; if the next cell on the left-to-right downward diagonal is occupied, place the next number in the cell immediately above the one last filled; after filling the cell in the lower right-hand corner, place the next number in the cell immediately above* "

Of course, like our young officer onboard the frigate "Lossen", we could as well have started in the middle cell of the top row, or even in the middle cell of the left-most or the right-most column. [18]

Inspired by the way in which the sequence of integers was assigned to the cells, Babbage visualized a path or a route of increasing integers through all the cells of the magic square. From this point of view there was no difference in principle between the assignment of cells in the magic square and the standard move of a chessman in the Knight's tour. The two approaches shared the common property that the finite collection of cells in a square, was assigned a sequential ordering defining a unique path. This, I would suggest, is the fundamental operation which Babbage intuitively related to the exposition of transposition ciphers in Bishop Wilkins' cryptographical treatise.

The basic problem in all these cases, was simply to let a string of text follow a predefined path through the finite number of cells in a square, or even a rectangle. Definitely, it was as evident to Babbage as to any modern reader, that in this sense the magic square and the knight's tour simply added to the number of devious routes envisaged by Bishop Wilkins. That this indeed is common knowledge in our time, is brought out in the following remark by Helen Fouché Gaines in her admirable instructive book *Cryptanalysis* from 1939: [19].

"The most popular of the geometrical figures appears to be the square ... Any device or game, which will provide a square, is likely to be seized upon as the source of a transposition key. We find two widely-known examples of this in the magic square *and the* knight's tour."

Whether this was equally well known in Babbage's days I have not been able to ascertain. But it is known, as pointed out in 1871 in the anonymous article [20]) in MacMillan's Magazine, that transposition ciphers *"are not so common as the former classes* (substitution), *although some of them possess considerable merit"*. Yet, what is significant here, is the attempt to come up with a mathematical formulation.

Babbage's intuitive understanding of the potential possibilities of the geometry of situation and his declared intention to explore them, were put into writing about 1822. Only eleven years later, in 1833, the famous Gauss wrote: [21])

"Of the geometry of position, which Leibnitz initiated and to which only two geometers, Euler and Vandermonde, have given a feeble glance, we know and possess, after a century and a half, very little more than nothing."

In spite of this complaint Gauss himself did not contribute to the discipline. True, he did encourage his students to develop the topic, resulting in the important contributions by Listing and Kirchhoff. But the point was that, although in principle it was obvious what had to be done, the problem how to do it appeared unsurmountable. The necessary tools simply did not exist.

However, to appreciate the deeper significance of the challenge which Babbage attempted to meet, let me go back in time to Descartes' publication in 1637 of his *Discours de la méthode pour bien conduire sa raison, et chercher la vérité dans les sciences*, or discourse on the method of good reasoning, and searching for truth in the sciences. A classic of literature and philosophy, this book contains among its three appendices his only work on mathematics, the celebrated *La Géométrie*, which introduced his ideas on coordinate geometry and algebra. Apparently the latter work was also in Babbage's library in an edition of collected works printed 1663, since Tucker's catalogue lists the other two appendices as examples of the contents. So perhaps Babbage would have accepted a modern view as follows. [22])

Today, the use of Descartes' (and Fermat's) coordinate or analytical geometry is taken almost for granted. It is commonplace to prove, with the aid of algebra, any number of facts about curves or other geometrical objects, but also the method of approaching the problems is almost automatic. Coordinate geometry provides a classification of geometrical problems and the quantitative tools to deal with them. Indeed, as expressed by Descartes, the invention combines the best of algebra with the best of geometry. Geometric concepts can be formulated algebraically and geometric goals attained through algebra. Conversely, by interpreting algebraic statements geometrically one can gain an intuitive grasp of their meaning as well as suggestions for the deduction of new conclusions.

By analogy to this view of coordinate geometry the obvious point, recognized at least intuitively by Babbage, as well as by Gauss, was that, to make a geometry of relative position useful and systematic, an associated algebra needed to be developed. The difficulty, however, was the problem of inventing an algebraic interpretation suitably oriented towards the novel situation.

Cartesian space, the coordinate geometry conceived by Descartes, determined its associated algebra by its metrical properties like distance and angle. In fact, the *binding property* turning the set of points into a geometrical space, was that of distance. Because, in two or higher dimensions, distance, conceived as a straight line between two points, provided the unique link with the associated algebra by means of the famous theorem of Pythagoras, or its higher dimensional generalizations.

In topology or geometry of situation, distance and angle are irrelevant. All metrical relationships have been substituted by properties of relative position. The two-fold problem therefore arises:

– What is the binding property *geometrically* relating two points of the point set of relative positions?
– How is the binding property expressed *algebraically* in terms of the associated "coordinates" of position?

Clearly, the answers to these two questions will establish the necessary breakthrough towards a geometrical formulation of the notion of relative position and its associated algebraic interpretation. Babbage's intuitive attempt in this respect, is not without merit.

Dealing with „games of skill" it should be recognized that Babbage makes the tacit assumption that the point set of relative positions is *finite*. According to Dubbey he then states the basic mathematical problem as follows: [3])

"The first object is to discover some method of expressing any one indifferently out of n *quantities or positions and when this is abstracted to express any one indifferently out of the remaining* n-1."

Mapping the game of tic-tac-toe upon the finite geometrical space of a magic square, Babbage demonstrated that the logical consequence of this plan, was a path through all the cells in the square.

In a following section, we shall relate the problem of relative positions in a finite space to the notion of data arrays in APL. Here, therefore, it will suffice merely to indicate a modern interpretation of the direction of Babbage's work. From this point of view two things in particular come to mind.

First, Babbage's plan suggests that *order* may be the binding property relating points of relative position. Especially, his approach has a distinct similarity to Cantor's much later concept of *well-ordering*. Namely, that each non-empty subset of points has a first member.

Secondly, since his point-set is finite, the property of well-ordering opens up for an arrangement of all points in a single path, determining a *total order*.

Of course, these two results of fundamental importance are only implicit in Babbage's approach. Yet, the fact that they subconsciously guided him, bespeaks his remarkable intuition. On the other hand, I very much doubt that he attached explicit significance to the underlying notions. His greatness as a scientist was in the general area of systems engineering rather than in mathematics. An indication that he perhaps suspected this himself, is his display of eccentricity at Cambridge in connection with his passing the University Senate House Examinations, popularly known as the Tripos, for the Bachelor of Arts degree. In the words of Becher [9], Babbage, *"believing that he could not best Herschel and Peacock in the Tripos, .. refused to compete for mathematical honours, thereby losing stature and influence"*. In 1813, therefore, Babbage obtained only a non-honours degree whereas his two friends, Herschel and Peacock, became senior and second wrangler, respectively.

In the late 1840s, Babbage returned to the question of magic squares and games of skill, but this time from the new angle of designing an automaton for this purpose. In addition to the popular account given in his *Passages*, he left an entire file of rather extensive notes and flowcharts on game strategies, and engineering sketches among his scientific papers in the British Library. [23]) As even a superficial perusal will show, much of this material anticipates the modern development in the area now modestly known as *artificial intelligence*. However tempting it may be to disgress into a discussion of this contribution of Babbage, this is a very different story – perhaps to be told by somebody else. Though, I cannot refrain from mentioning two titles in Babbage's library, which relate to his revived interest in the field.

One is a French treatise by B. Violle from 1837: *Géometrie. Traité complet des carrés magiques, pairs et impair, simples et composés, &c., suivi d'un traité de cubes magique, et d'une essai sur les cercles magiques*, (or, Geometry. A complete treatise of magic squares, even and odd, simple and composite, etc., followed by a treatise of magic cubes, and an essay on the magic circles). Apparently Babbage made a rather thorough study of this work, for his notes even contain illustrations removed from the book.

The other work is Daniel Milford Peacock's *Treatise on Algebra. Vol. II.: On Symbolical Algebra and its Applications to the Geometry of Position*. Published 1845 by a namesake, but no relative of Babbage's friend, the acquisition of this book may indicate Babbage's never failing interest in the problem he attacked more than twenty years earlier. But it may also have been more than just professional curiosity. For in 1816 D. M. Peacock, an ardent adherer of Newton's notation, wrote a penetrating criticism of the translation of Lacroix's differential algebra, published by Babbage and his friends to promote the differential notation of Leibnitz.

2.4 Geometrically Speaking

To attain precision and yet cope with complexity, is a general problem in computer applications. The trade-off between flexibility of syntax and power of operation in the design phase of the programming language to be used, determines its solution. In the period of developing the modern computer the emphasis was almost exclusively on grammar. This was a natural consequence of the constraints at the time, particularly in hardware, establishing the *scalar:* the single number or the single character (letter), as the fundamental data element. The danger of this constrained view, however, is that it neglects, and even runs counter to the general view of powerful operations and simple syntax, developed over the past century in mathematics and adopted with impressive results in all the pure and applied sciences based on this discipline.

Alfred North Whitehead, who over the years 1910-1913 wrote the famous *Principia Mathematica* together with his pupil Bertrand Russell, eloquently brought out the significance of the mathematical view: [24])

> *"By the aid of symbolism, we can make transitions in reasoning almost mechanically by the eye, which otherwise would call into play the higher faculties of the brain. It is a profoundly erroneous truism, repeated by all copybooks and by eminent people when they are making speeches, that we should cultivate the habit of thinking of what we are doing. The precise opposite is the case. Civilization advances by extending the number of important operations which we can perform without thinking about them."*

Basically, the economy of thought attained in the mathematical operations, is brought about by incorporating complexity into the data objects. Inspired by man's geometrical perception of things, complexity was embodied in the structure, organizing the data objects according to pattern: Lists, tables, or even boxes of data. Such data objects, which here I shall call *tabular arrays*, are the main concern of mathematical topics like determinant theory and matrix algebra. Of course, the scalar or single datum is included among the tabular arrays, but now as the special case devoid of geometrical structure.

But mathematical abstraction is also flexibility of thought. To attain precision in the face of complexity, mathematics provides an astonishing new interpretation.

Namely, that we may think of an entire class of tabular arrays as representing, under certain prescribed conditions, just a single geometrical object. The elegance and power of this unexpected change of view is that we may now endow this abstract geometrical object with any property of our fancy, completely independent of any reference frame. By analogy, as suggested by Gabriel Kron in 1939, we may compare the abstract object to a marble statue or a steel frame, and the associated class of tabular arrays to mathematical "photographs", each taken from a different view [25]

Vector algebra, originating in the well known parallellogram law for addition of forces and velocities in mechanics, is the classical theory developing this point of view. The abstract object called a vector, is depicted in n-dimensional space as a directed arrow. In any given reference frame its algebraic representation is a list of n coordinates, a socalled *n-tuple*. It is important to note that, as we go from one reference frame to another, the coordinates themselves may change, but their formation into a list is preserved

However, just before the turn of our century it was realized that there were certain fields of physics, like elasticity, which were forced to introduce entities of a new kind, more complex than vectors. When we study the 3-dimensional stresses or tensions in the interior of a deformed body, we discover a collection of six numbers, inseparable one from the other, which behave like the six components of a certain new quantity. Physicists, puzzled by the fact that there was six rather than three coordinates, hesitated for a long time to give name to this entity. Yet the study of the physics of crystals revealed the existence of a great number of analogous cases. In his remarkable treatise *Lehrbuch der Kristallphysik* from 1910, W. Voigt, the great crystallographer of Göttingen, was the first to recognize the kinship of these various quantities by insisting on their common character, and baptizing them "*tensors*" [26] in recognition of their origin in the question of tensions or elastic stresses. Since then, the idea of a tensor has become classic, giving rise to a mathematical tensor algebra of considerable importance in physics and engineering

As geometrical objects tensors are so abstract in their mathematical nature, that no one has been able to draw a simple picture of them, like the directed arrow representing the vector. Still, from the engineering viewpoint of performing numerical calculations with them, Kron advocated in his book from 1939 a brilliant approach, depicting tensors in terms of tabular arrays. [25] Depending on the rank of the tensor he simply organized its components (coordinates) in a tabular array of a corresponding number of dimensions. Thus, the stress tensor originally dealt with by Voigt, was depicted by a 3-by-3 table of components with zeros in the main diagonal (from upper left to lower right), corresponding to the fact that it was of rank 2. Similarly, a vector, now interpreted as a tensor of rank 1, preserved its form

as a list of components. Even more remarkable, Kron generalized the tensorial approach introducing a novel organization of the tensor components in the form of *nested arrays*. That is, hierarchical array structures in the sense that elements of an array may themselves be arrays, continuing the process in depth.

Now, the purpose of this rather long explanation was simply to bring across an idea which we shall borrow from the mathematicians. Namely, that a tabular array, under some conditions, may be interpreted as a "mathematical photograph" of an invariant geometrical object. Our purpose is to attempt to capture more precisely, in the context of APL, the nature of the invariant properties of such abstract objects. Because only in this perspective it will be possible to bring together in APL the three topics of interest in Babbage's Philosophy of Analysis: Notation, permanence of form, and topology or geometry of relative position. In this study, we shall forego everything about vectors, tensors, or even nested arrays. In fact, let us take our starting point in the down-to-earth problem of reading and writing

2.5 It Began With ABC

The word *alphabet* derives from the names of the first two letters in the Greek alphabet: *alpha* and *beta*. The invention, however, was not Greek but Phoenician. The peculiarity of the Phoenician form, inherited by all Semitic alphabets, was that all symbols stood for consonants only. This was changed by the Greeks who altered some of the letters to vowels, simultaneously adding a few more letters. Of the many early varieties the Ionian-Milesian alphabet, officially adopted in Athens in antiquity, [27] is the form recognized today as the Greek alphabet. All Western alphabets are derived from this, usually by way of the Latin alphabet.

Perhaps the most important property of an alphabet is the established sequence of the twenty-odd letters. Mathematically speaking, an alphabet is simply a list of distinct symbols in a fixed order. That is, there exists a one-to-one correspondence between the sequence of n letters in the alphabet and the sequence of the first n positive integers. Since the positive integers are *well-ordered* in the sense that each non-empty subset contains a smallest number, so are the alphabetic letters. An alphabet, therefore, may be conceived as a representation of an *ordinal scale* as an alternative to the sequence of positive integers. The great convenience of dictionaries and telephone directories, which the Chinese with their ideographic characters do not enjoy, illustrates the importance of this interpretation.

The first to recognize this numbering quality of the alphabetic letters were the Greeks. To begin with, they simply numbered the letters *alpha* through *omega* by the sequence of ordinal numbers 1 through 24, respectively. Later, expanding the alphabet to $27 = 3\times9$ letters, they mapped it to a new sequence, so that each group

of 9 letters would represent the units, the tens, and the hundreds, respectively. The importance of this step was that they went from an ordinal to a cardinal number representation. Whereas before the letters could only be ordered with respect to each other, they could now also be added together. In fact, Greek mathematicians such as Archimedes and Diophantus used these alphabetical numerals for computation.

This gave rise to the study of letter or word calculations, *gematria*, as it was called by a corruption of the Greek word *geometria*. [27]) For example, writing in Greek the early Christian scholars would give the value 99 to the word "Amen":

$$\alpha\ \mu\ \eta\ \nu = 1 + 40 + 8 + 50 = 99$$

since the four Greek letters were assigned the following values: *alpha* = 1; *mu* = 40, *eta* = 8; and *nu* = 50. At the end of a Greek prayer, therefore, this word would often be written

$$\text{ϙ}\ \theta = 90 + 9 = 99$$

because the (additional, but not now used) letter *koppa* = 90 and the letter *theta* = 9.

This association of cardinal numbers with letters strongly appealed to human imagination. Persons or things the letters of whose names had the same total numerical value, were also thought to be mystically related. In medieval times, the outcome of duels would be "calculated" from the arbitrary sums of the letters or digits in the combatants' names, predicting the winner the one with the larger sum. Reversely, names were often believed to underlie numbers. For instance, there can be little doubt that a name is implied in the famous quotation from the *Book of Revelations* (13:18).

> *"Let him that hath understanding count the number of the beast: for it is the number of a man; and his number is Six hundred threescore and six"*

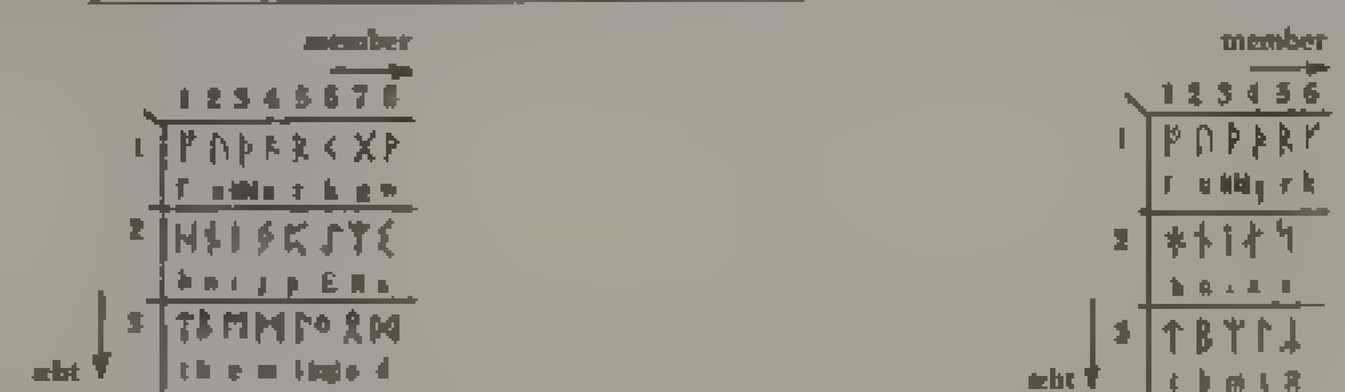
Toying with problems of this nature, Michael Stifel, who died 1567, valued his "word calculation" above his really important contributions to mathematics, referred to by Babbage in his discussion of notation. Even Newton considered his *Principia* from 1687 far less significant than the religious inquiries of this nature in his two books: *Chronology of Ancient Kingdoms Amended*, and *Observations upon the Prophecies of Daniel and the Apocalypse of St. John*

At the tercentenary of Newton's birth in 1942 (postponed by World War II to 1946), Lord John Maynard Keynes, the economist who was then Chancellor of Cambridge University, contrasted the conventional impression of Newton as *"the first and greatest of the modern age of scientists, a rationalist, one who taught us to think on the lines of cold and untinctured reason"*, with the following personal view *"as his own friends and contemporaries saw him"*: [28])

> *"I do not see him in this light. I do not think that anyone who has pored over the contents of that box which he packed up when he finally left Cambridge in 1696 and which, though partly dispersed, have come down to us, can see him like that. Newton was not the first of the age of reason. He was the last of the magicians, the last of the Babylonians and Sumerians, the last great mind which looked out on the visible and intellectual world with the same eyes as those who began to build our intellectual inheritance rather less than 10,000 years ago. Isaac Newton, a posthumous child born with no father on Christmas Day 1642, was the last wonderchild to whom the Magi could do sincere and appropriate homage".*

In Northern Europe, going some thousand years back in time, it was not the cardinality of the numbers associated with the letters that spurred the imagination. It was the order and the geometrical pattern derived from that order. Because the amazing fact about the *runic* alphabet is that it was ordered in 3 separate sublists rather than in a single list. Indeed, the way it was used in Scandinavia suggests that it was conceived as a *table*, although no runic inscription has been found to confirm this view.

The old Germanic runes, originally 24 in number as shown in figure 12A, seem to be derived some time during the first three centuries A.D. from one or more of the classic alphabets, such as Etruscan, or possibly from some northern Greek colony. [29]) Yet, whatever their origin, the shape of the letters had clearly been adapted for easy cutting in wood or stone rather than for use on wax tablets or parchments. All horizontal strokes were drawn at an angle, as in the runic A and F, so that they would not run parallel to the grain of the wood, and the curved lines were either made straight or broken, as in the runic O. In Scandinavia, at the beginning of the Viking Period about 800 A.D., a new abbreviated form of only 16 letters is encountered. As demonstrated in figure 12B, the new alphabet adopted no less than ten of the runes from the old alphabet.



A) The Pre-Viking Form of 24 Letters. *B) The Viking Form of 16 Letters*

Figure 12. The runic alphabet or *futhark* (from the first 6 letters) was divided into 3 *æhts* (genders).

Two peculiarities characterize the development of the runic alphabet. First, the established order of the classic alphabets was given up for a new order, the first six letters of which, *f u th a r k*, gave the name to the runic alphabet. Secondly, the letters were grouped into three *æhts* (genders), to use the original Anglo-Saxon term. [30]) In general, as illustrated in figure 12, each runic letter was therefore identified by a pair of ordinal numbers or coordinates: The number of the æht, and the number of the member within the æht. Since many finds depict the runes by some representation of such pairs of coordinates, this seems to indicate a tabular conception of the futhark.

Various reasons have been proposed to explain these peculiarities of the runic alphabet. One is that the runes were used originally for casting lots and telling the future, rather than for the purpose of actually writing. The historical evidence usually quoted in this connection, is the description of the customs of the earliest Teutons in chapter X of the monograph *Germania* published 98 A.D. by the Roman historian Publius Cornelius Tacitus. However, in the commentary of a recent translation, [31]) N. W. Bruun and A. A. Lund have pointed out that if in fact Tacitus had conceived the scratches in the wooden sticks as runes, he would have used the term "letters" (Latin: *litterae*) rather than the term "signs" (Latin: *notae*). Yet, as we shall see later, the latter term may have been used if the runes were conceived as enciphered letters.

Another explanation may be that the runic letters were assigned symbolic names associated with some magic content, as we have seen was the case for the numbers assigned to the Greek alphabet. The recording of the runic letters, therefore, was dependent upon this magic content. [27]) For instance, the Greek letter *theta* became *thurs* (preserved in the word Thursday), implying *Thor*, the Old Norse god of thunder and battle. Conceived as a curse, it was therefore an evil rune, always bringing bad luck. Consequently, a magic spell could be cast "scratching" runes, which in turn could be broken erasing the incised runes. In the Elder Edda, a collection of Old Norse poems, this is brought out in a nutshell in the song about Skirner's Travel: [32])

"Thurs" jeg rister dig og tre stave:
"Horgal", "Halvgal" og "Higende"!
Men af jeg rister, som ind jeg rister,
ifald jeg det finder for godt

which has been rendered in English: [27])

I scratch a "Thurs", and then three runes
"Lust", "Sorrow", and "Pangs of Love"!
I scratch them out, as I scratched them in,
when they were needed

There is no need, however, to over-stress the magical significance of the runes. Nor should we deduce that runes were a form of writing specially associated in some way with monumental inscriptions. For it is not likely that anyone would learn the art of writing simply in order to carve inscriptions on tombstones. The fact that so many were carved, implies that in Viking times there were a fair number of people around sufficiently literate to read them.

Indeed, the excavations in Bergen after the fire in 1955, of about 550 inscriptions on wood from the early Middle Ages, have documented beyond doubt that runic communications: Labels on goods, trade documents, military orders, political messages, and private letters, were a necessary adjunct to the daily life in Scandinavia. [33]) To be sure, a message on a wooden stick: *"Gyda tells you to come home"*; a verse on a bone from the broth: *"Here is now but din and dispute"*; or another verse on a delicately cut piece of wood: *"Like you are, I would like my* [wife] *were"*; all from about 1200 A.D. and found at the site of the local inn, countermand in a rather profane manner the usual impression of magic and tombstones. Some of the Bergen inhabitants were even literary as exemplified by the runic quotation: *"Love conquers all, let us submit to love"*, from the Roman poet Vergil. The amazing fact is that the systematic excavation of just this single site almost doubled the number of known runic inscriptions in Norway. Clearly, this suggests that innumerable additional wooden inscriptions must have existed and been destroyed over the centuries. [34])

Usually, the Viking Period is dated from 793-1042 A.D. bracketed between two events: The destruction of the Lindisfarne Monastery, and the death of Hardicanute, the last Anglo-Danish king, after a drinking bout at a wedding. In error by more than a century, the Bergen finds merely explains the modern view of Viking literacy, deduced from archeological excavations in recent times. Perhaps in this respect, a most convincing indication of a widespread communication in written form is the superior ability in planning and organizing, and the impressive technological skill which enabled the Vikings to carry through military projects on a vast geographical scale. A brief mention of the construction work undertaken to fortify Denmark about 980 A.D., will illustrate the point. [35])

Apparently, the purpose of this project was to consolidate the central power of King Harald Bluetooth who claimed, on a runestone at Jelling for his parents King Gorm the Old and Queen Thyra, that he was *"the Harald who won all Denmark and Norway, and made the Danes christians"*. The construction work comprised rebuilding and extensions of *Dannevirke*, a thirty kilometer long system of fortified walls along the German border; improvement and building of roads and bridges, such as the one kilometer long bridge over Ravning Enge near Jelling, estimated to carry a maximum load of 5 tons; and the establishment of four ring-fortresses: *Aggersborg*

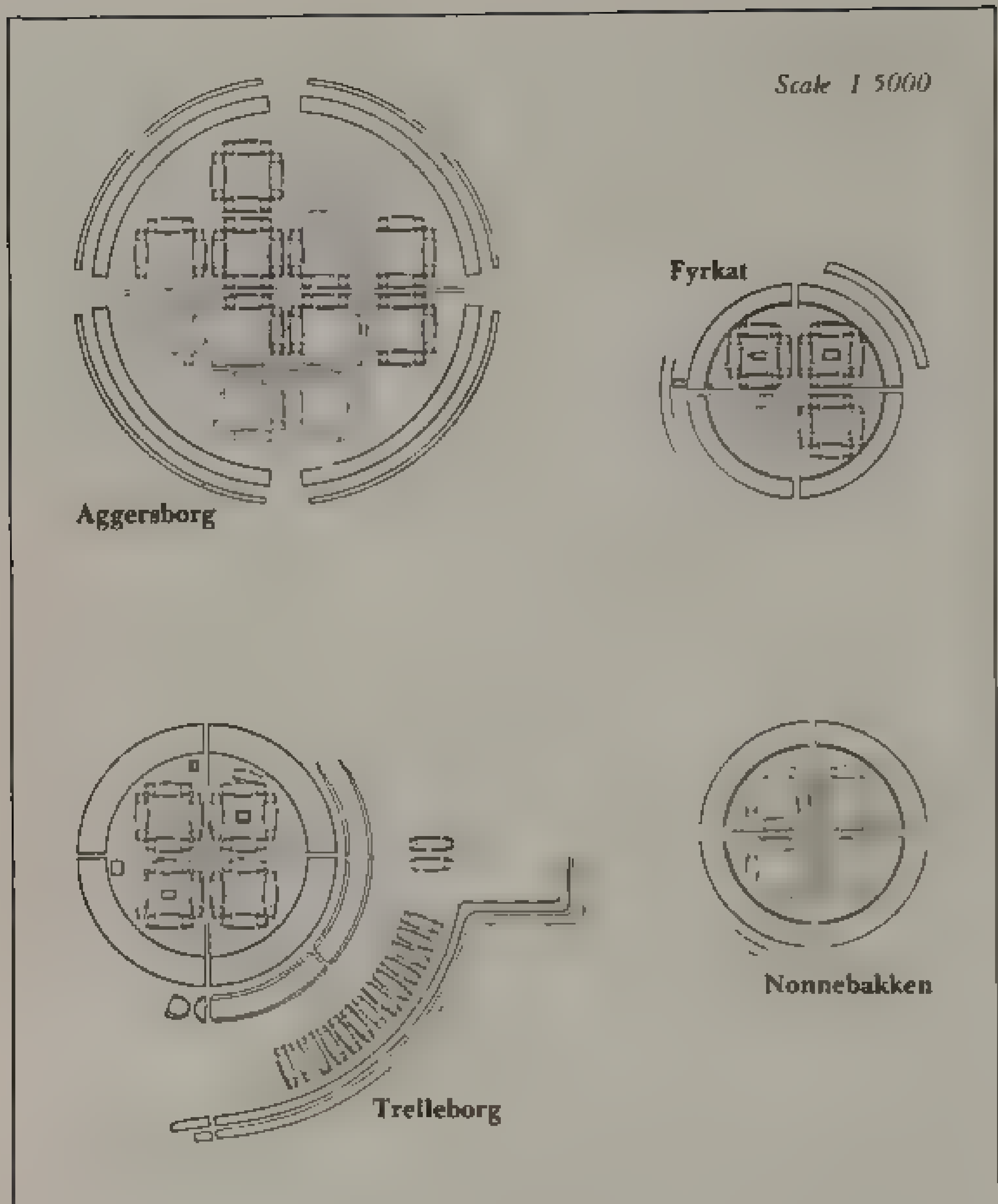


Figure 13. Ground-plans of the four Viking fortresses excavated in Denmark. Dotted lines indicate hypothetical reconstructions
Courtesy Dr. Olaf Olsen, Keeper of National Antiquities, Nationalmuseet, Copenhagen

and *Fyrkat* in Jutland, *Trelleborg* on Zealand, and *Nonnebakken* (buried under the city of Odense) on Funen.

Figure 13 shows the layout of these ring-fortresses. An impression of the size of the former three may be gained from the inner diameters of the yard which in order are 240 meters, 136 meters, and 120 meters, respectively. The ditches are from 4 to 18 meters wide and up to 5 meters deep. The earthen walls are from 11 to 19 meters thick and about 5 meters high. At the time, they must have been even higher, standing very steep and covered all the way down by a palisade of heavy oak timber. Actually, the standard unit length used in the construction was the Roman foot. For instance, the length of the houses (shaped like boats) was about 100 Roman feet, or approximately 30 meters. It has been estimated that together the four fortresses could garrison 5-6000 men; though in their short span of life, 20-25 years, the actual garrisons were significantly smaller but simultaneously included many artisans besides women and children.

To level the sites and create these earthworks of perfect geometrical precision did not only cost tremendous labour, but it must also have required a fair degree of mathematical knowledge and engineering skill. The actual design appears to be original to the Danish Vikings. It has therefore been suggested that they learned the necessary geometry and means of applying it from their contacts with the Byzantine Empire and the Arab world. However, even if mathematical learning was on its lowest level in Europe during the years 500 to 1400 A.D., European universities did teach enough of Euclid to supply this knowledge. It was not pure chance that Saint Thomas Aquinas' *Summa Theologiæ*, written about 1260, earned by its organisation the title of the "spiritual Euclid". Besides, if the knowledge had been acquired in Europe, it would explain the use of the Roman foot as unit length.

Irrespective of origin, however, the point is that there must have existed an educated class of Vikings combining literacy with an understanding of geometry. Indeed, as we shall now see, this combined interest has its roots in a long tradition of playing with geometrical patterns arising from the "scratching" of runes. Today, we would characterize it as secret writing. Yet, since apparently the different forms of ciphers were recognized and read in general by the literary part of the Viking community, the purpose must have been to conceal the messages from the gods rather than from human beings – a sort of Viking euphemism, or magic. Whatever the reason, the Vikings and their ancestors, the old Norsemen, delighted in the art of secret writing.

In their authoritative work from 1942 on Danish runic inscriptions, Jacobsen and Moltke list five kinds of, what may be called, *cipher runes* (Danish, *lønruner*). [36] The first of these, referred to as a systematic list of *abbreviations*, counts rather as a shorthand than as a cipher. Of the remaining four, the most rare is a monoalpha-

betic substitution based on the *Cæsar alphabet* discussed earlier. Apparently, three versions have been found, corresponding to a cyclic shift to the following letter, to the preceding letter, and to the letter before the preceding letter, respectively, of the futhark conceived as a list.

The only known Danish find of this cipher illustrates the first mentioned version in terms of the youngest futhark from 800 A.D. or later (see figure 12B). It is noteworthy, that this find completely agrees with several Swedish inscriptions, for example the one on the famous Rök stone, reported by Jansson. [29]) It may therefore well be that the source of inspiration was one of the second century A. D. Roman authors: Gajus Suetonius, Aulus Gellius, or Dio Cassius. As quoted by Lindenfels, [37]) each of them described in detail this technique, called by Suetonius "*per notas scribere*" or writing through signs. When therefore Tacitus used this term for the runes, it was perhaps because he considered them as enciphered letters.

Two of the remaining kinds are simple transpositions. One is *anagramming* of words, reordering their letters such that a magic word, say, *agla*, is written *gala* or *laga*. Liestøl, in his discussion of the Bergen finds [35]) relates runic anagramming to the type of superstition whereby difficult problems are posed to occupy the powers of evil who are then caught finding the solutions to be powerful words of magic. Infallible in this respect was the inscription going back to heathen days:

mtpkrgbmmmssssssttttttaaaalldttl

because in a single formula, seven names were tied together: mistil, tistil, pistil, kistil, ristil, gistil, and bistil. The first of these names is the mistletoe, a plant of central importance to magic through times. It will be noted, that to give the evil spirits a sporting chance, the anagramming is not entirely random. Thus, the formula consists of six letter groups the first of which contains all the initial letters in order, etc.

When Newton in a letter of 24 October, 1676, communicated his differential calculus, called the *method of fluxions*, to Leibnitz, he did not give him even this chance. [38]) Newton's anagram was perfectly randomized: "*6a 2c d æ 13e 2f 7i 3l 9n 4o 4q 2r 4s 9t 12v x.*" In fact, had Newton not yielded, in a letter of 27 August, 1692, to an urgent request by Wallis for a solution, subsequently published by the latter, we would never have known that this jumble of letters was supposed to mean "*Data Æquatione quotcumque, fluentes quantitetes involvente, fluxiones invenire, et vice versa*", - given any equation, involving fluent quantities, to find the fluxions, and vice versa. But back to the cipher runes.

Another transposition method used in runic inscriptions was the the *word reversal*. That is, the text has to be read from right to left like the execution of an APL statement. This technique appears to be rather old. Thus, in their attempts at interpreting inscriptions on weapons or silver jewelry dating back to about 200 A.D.,

Scandinavian archeologists as a matter of routine read the texts (usually names of owners or makers) from both left and right as they perform the linguistic analysis. A possible explanation of the origin of the method may be that some artisans stamped their names on their products as a kind of workshop guarantee.

The last and most advanced technique used in runic inscriptions was a substitution cipher, the so-called *checkerboard*, which is also known as the *Polybius' square* after the Greek historian who described it in the second century B. C. Its basic idea is to scramble the alphabet in some random order, arrange it in a square (rectangle), and then represent each letter by the pair of corresponding coordinates giving its row number and column number. In cryptography, this is a standard method for substituting letters by numbers. The ancient conception, subdividing the futhark into three æhts, clearly invites an application of the checkerboard, if it was not inspired, in fact, by this cipher. Here, however, the Vikings introduced a curious twist, in that the first axis of coordinates was reversed, interchanging the first and the third æhts.

Having no proper number system, the Vikings invented a variety of fancy signs to represent the coordinate pairs of the futhark checkerboard. Figure 14 A-C provides a few illustrations from Sweden and Norway, all referring to the 16-letter futhark with the æhts in reversed order. Typically, the cipher was applied only to parts of the inscriptions like an author's signature on the Swedish Rotbrunna stone. Here, the æht is indicated by long strokes and the member within the æht by short strokes. The following coordinate pairs are distinguished: 2,4; 2,3; 3,5; 2,3; 3,6; and 3,5. Entering figure 12B, numbering the æhts from the bottom upwards, we find that the name is *airikr* or Erik, as we would spell it today.

Figure 14 A. Rotbrunna Stone, Uppland, abt. 1000 A D

The crosses on the Swedish Rök stone serve the same purpose as the strokes. The slash from upper left to lower right gives the æht, while the converse slash from lower left to upper right is the member in the æht. The crosses are read in sequence from left to right, but each cross is read like a table, first the pair of upper arms, and then the pair of lower arms. The initial two letters are therefore *si*, specified by the coordinate pairs. 2,5 and 2,3 for the leftmost cross. The two small runes at the top of the first cross represent a non-enciphered variation of the 16-letter futhark, supposed to read *bi*. Hence, the first word is the name *Sibi*, an abbreviation for Sigbjørn.

Figure 14 B. Rök Stone, Östgötland, abt. 800 A.D

The Bergen cipher runes are characterized by their mirror or bilateral symmetry about a vertical center line [39]) The æht is denoted to the left of this line, and the member within the æht to the right. The runes are enciphered by means of the 16-letter Viking checkerboard, with the first and third æhts interchanged as usual According to Liestøl,[35]) the three samples in figure 14C can be explained as follows.

The upper wooden stick is unusual since in one inscription it combines cipher runes of three different kinds: fish, shells (known technically as double or mirror "th"s), and twigs. Two ordinary runes: "s"and "i" are interspersed with the cipher runes. Liestøl reads the first nine cipher runes as follows:

Coordinate pairs:	36	32	33	36	23	31	23	34	s.
Interchanging æhts:	16	12	13	16	23	11	23	14	s
Plaintext letters:	k	u	(th)	k	i	f	i	a	s
Pronounciation:	G	u	ð	g	i	f	i	o	s
English:	G	o	d	g	i	v	e	u	s

The middle illustration has four cipher runes shaped as men with twigs hanging down from their arms. Counting only the number of twigs, we read: 36 14 23 13 or "Klim", which is the first four letters of the name Klement. So, obviously the writer is entreating St. Clement.

Finally, the last stick depicts forkbearded faces (of holy men?) "Splitting hairs" it reads: 25 23 13 14 23 12 23 : 25 23 22 32, which Liestøl interprets as "sim libi sinu", meaning "som livet sit" or, in English as one's life. Unfortunately, the stick is broken so the rest of the inscription is lost

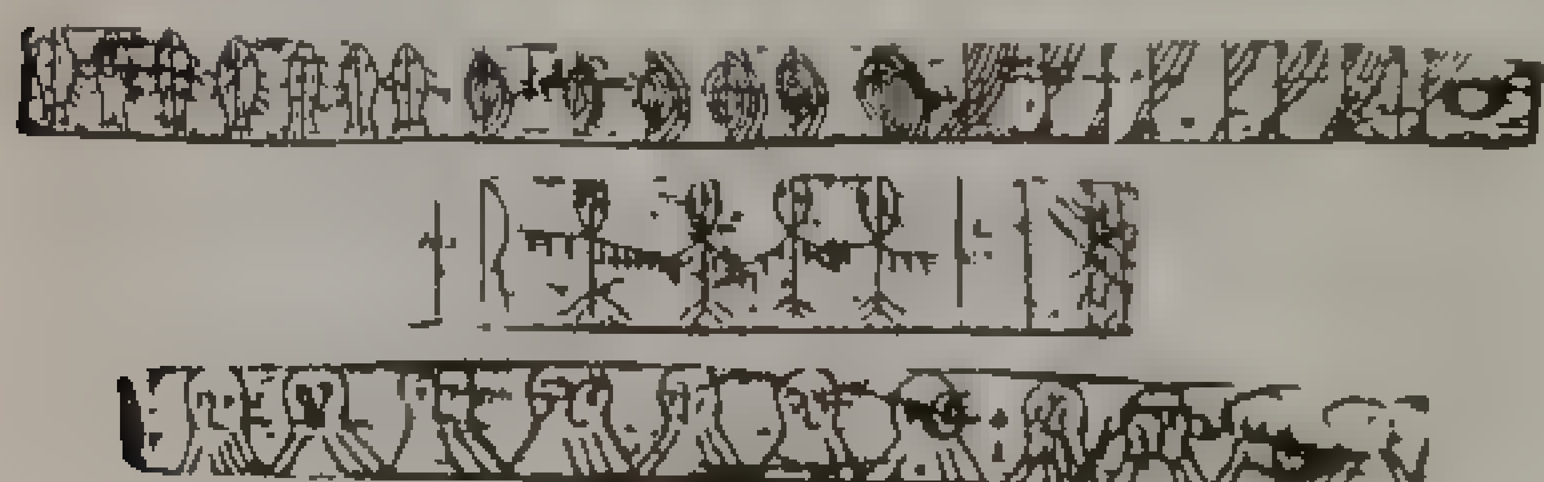


Figure 14 C. Wooden Amulets, Bergen, 1100-1200 A D

(A. Liestøl; Copyright Universitetets Oldsaksamling, Oslo)

2.6 Metric Versus Non-Metric

Comparing the different kinds of cipher runes with the enciphered advertisements from the agony columns, collected by Babbage to illustrate his book, one finds no difference in principle. Even the checkerboard alphabet enjoyed a popularity in Victorian London comparable to that among the Vikings. To illustrate, I have reconstructed in figure 15 the tabular form of a cipher alphabet, unravelled from an enciphered advertisement by Babbage. Listed in a note [40]) dated 13 September 1833, the plaintext letters were substituted by two-digit ordinal numbers from 10

```
IN FOLIO 17, DATED 13 SEP 1833, BABBAGE LISTED
THE NUMERICAL CIPHER ALPHABET

     A  B  C  D  E  F  G  H  I  J  K  L  M
    10 22 24 26 12 28 30 32 14 .. 11 13 15
     N  O  P  Q  R  S  T  U  V  W  X  Y  Z
    17 16 19 .. 23 25 27 18 29 31 .. 20 ..

GUESSING THE TWO-DIGIT NUMBERS TO BE PAIRS OF
INDICES OF A 3-BY-10 CHECKERBOARD, WE FIND

             \ 0 1 2 3 4 5 6 7 8 9
             +--------------------
            1| A K E L I M O N U P
            2| Y   B R C S D T F V
            3| G W H

EVIDENTLY, CONSIDERING THE ALPHABET
      ⍴⎕←APL
ABCDEFGHIJKLMNOPQRSTUVWXYZ
26

THE PATTERN IS TO MOVE THE VOWELS
      ⍴⎕←VOWELS
AEIOUY
6

TO THE FRONT  OF THE ALPHABET
      ⍴⎕←XYZ←VOWELS,(~ABC∊VOWELS)/ABC
AEIOUYBCDFGHJKLMNPQRSTVWXZ
26

AND THEN FILL IN THE CHECKERBOARD AS FOLLOWS
      ⍴⎕←3 10⍴(¯2 13⍴XYZ),4⍴
[illegible]
YGBRCSDTFV
GWHXJZ
3 10

THIS RECONSTRUCTS THE MISSING ENTRIES
```

Figure 15. A Checkerboard Alphabet of 1833, reconstructed from Babbage's notes. (BL., Add MS. 37205, F.17).

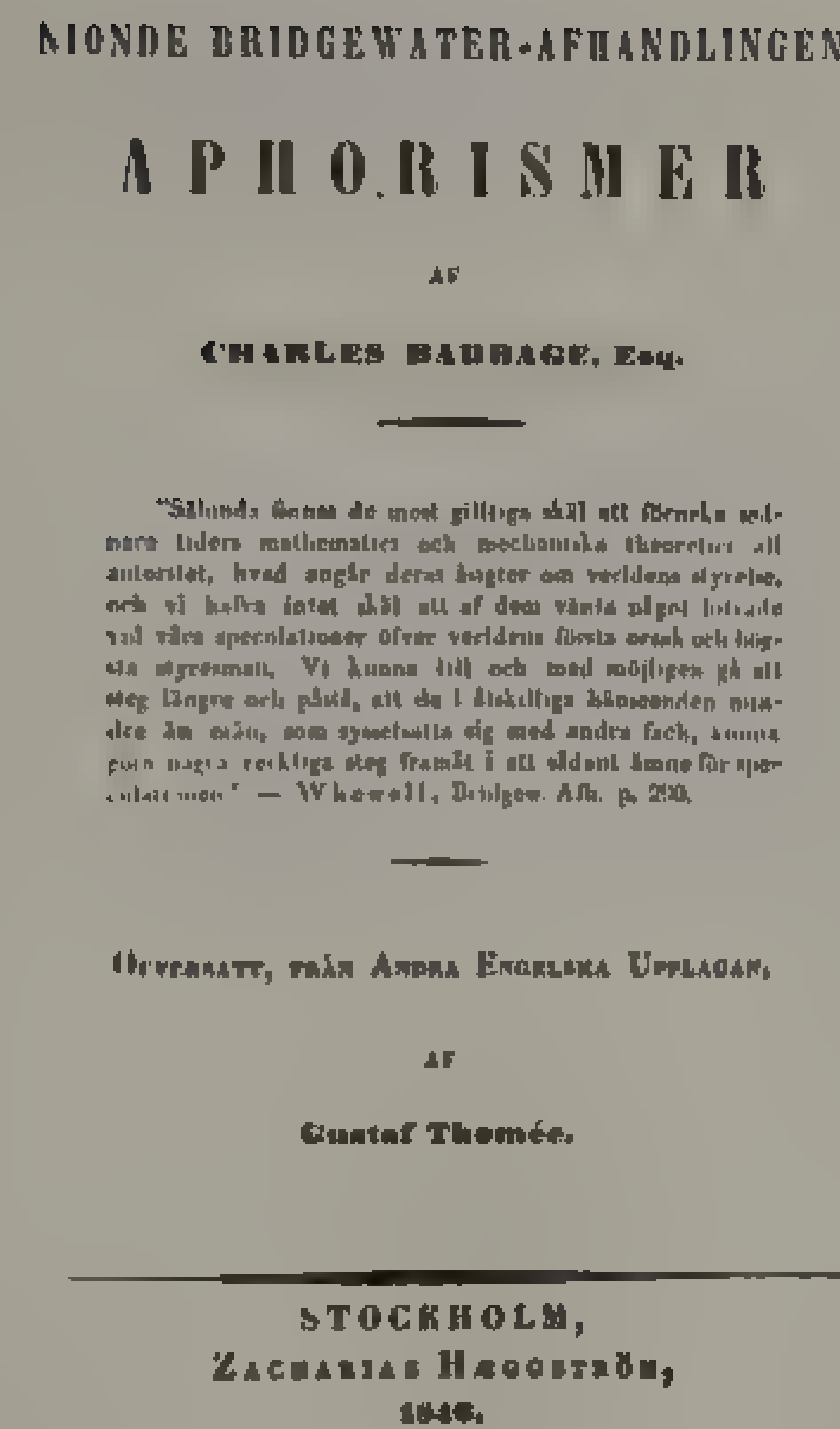
to 32, but with no numerical representation of the letters *I, Q, X,* and *Z*. What gave away this checkerboard was the number system which clearly corresponded to the coordinate pairs of a 3-by-10 rectangle, counting the rows from one and the columns from zero. The emerging pattern, filling in the known letters, immediately identified the representation of the missing four letters.

The agreement between the Viking ciphers and the Victorian ciphers, almost a thousand years apart, is thought-provoking. In between, of course, other and more sophisticated techniques had been invented. Yet, the fact remains that in ordinary practice, people of so different backgrounds as a Viking and a Victorian gentleman relied on the same intellectual principles.

Ideas which thus propagate, almost independently of the particular human background, must be rooted in some fundamental experience shared by mankind. Most evident in this respect is our perception of physical space. Here, intuitively, we can agree as to what we will consider a basic truth, perhaps even a law. Through history, the successful solution of complicated problems hinged on man's ability to invent suitable geometrical representations. Geometry, in its broadest sense, ruled the abstract thinking of man. It was therefore for good reasons that mathematics, when Babbage entered Cambridge University, formed the core of the liberal education. It also explains why so many 19th century British mathematicians were actually lawyers or country parsons by profession.

However, at the time Babbage and his friends brought the "analytical revolution" to Cambridge, the age in which the teaching of mathematics could be subordinated to other objectives of education without sacrificing mathematical skills, was at an end. As the curriculum expanded in the 1830s and 1840s, it became more and more difficult to provide within one program a liberal pre-professional education and also an education for mathematical careers. When therefore Babbage and the other reformers pushed on, promoting pure analysis to the extent of threatening to destroy the foundations of a liberal education, resistance built up.

The most vocal defender of the liberal education and critic of the analysis that had come to dominate the curriculum, was William Whewell, a Cambridge friend of Babbage's and a former member of the Analytical Society. [41] Whewell set forward his basic view on the subordinate role of mathematics in his *On Astronomy and General Physics*, the first of alltogether eight treatises, bequested by the late Lord Bridgewater to give evidence in favour of natural religion. Printing Whewell's offending statement on the title-page, Babbage counterattacked in a *Ninth Bridgewater Treatise*, which he added to the series at his own expense (see figure 16). On close terms, the ensuing controversy between the two men was carried on, to quote Hyman, [42] "*in the very best academic tradition, openly, trenchantly, and with high good humour*"


NIONDE BRIDGEWATER-AFHANDLINGEN.

APHORISMER

AF

CHARLES BABBAGE, Esq.

"Sålunda kunna de med giltiga skäl att förneka senare tiders mathematici och mechaniska theoretici all auktoritet, hvad angår deras åsigter om verldens styrelse, och vi hafva intet skäl att af dem vänta något bistånd vid våra speculationer öfver verldens första orsak och högsta styresman. Vi kunna till och med möjligen gå ett steg längre och påstå, att de i åtskilliga hänseenden mindre än andra, som sysselsätta sig med andra fack, kunna göra några verkliga steg framåt i ett sådant ämne för speculationer." — Whewell, Bridgew. Afh. p. 290.

Öfversatt, från Andra Engelska Upplagan,

AF

Gustaf Thomée.

STOCKHOLM,
Zacharias Haeggström,
1846.

Figure 16. Facsimile of the title page of the Swedish translation of Babbage's *Ninth Bridgewater Treatise*, Stockholm, 1846. Referring in particular to Laplace, the quotation by William Whewell was in the original: "*We may thus, with great propriety deny to the mechanical philosophers and mathematicians of recent times any authority with regard to their views of the administration of the universe; we have no reason whatever to expect from their speculations any help, when we ascend to the first cause and supreme ruler of the universe. But we might perhaps go farther, and assert that they are in some respects less likely than men employed in other pursuits, to make any clear advance towards such a subject of speculation*".

Whewell, professor at Cambridge and Master of Trinity, was a formidable opponent. A brief glimpse of his wit and elegance is revealed by the following contribution to ciphers, written at the request of a young lady: [45])

I 0 a 0 but I 0 U,
O 0 no 0 but O 0 me;
O let not my 0 a 0 go,
But give 0 0 I 0 U so.

Thus deciphered.
(You *sigh for* a cypher, but I *sigh for* you;
O *sigh for* no *cypher*, but O *sigh for* me·
O let not my *sigh for* a *cypher* go,
But give *sigh for sigh, for* I *sigh for* you so.)

Whewell was also a better politician, so in the end Babbage and his friends lost out. However, at the same time as he was undermining the increasing emphasis on pure mathematics, Whewell was successful in preserving the tradition conducive to the development of physics. Whewell regarded mathematics as a tool for solving physical problems rather than as something of intrinsic interest. He even urged that engineering be included in the curriculum. It is noteworthy that Whewell's view, that insight into the abstract concepts must be based on physical or geometrical interpretations, was shared by Stokes, William Thomson (Lord Kelvin), and Maxwell, the famous Cambridge physicists who led Britain to the forefront of research.

But let us not interpret this to mean that Babbage, Herschel, Peacock, and their friends were wrong in advocating the teaching of the abstract principles of analysis prior to its applications. Their view that pure analysis should be developed for its own value and beauty, rather than merely as a useful tool, was no less reputable. A few names selected from Babbage's circle of acquaintances will bring to mind some impressive contributions to logic and algebra giving merit to this viewpoint.

One was Augustus De Morgan, a long-time friend and supporter of Babbage's, who about 1840 became, perhaps at Babbage's instigation, the mathematics instructor of Lady Lovelace. [44]) Like Babbage, De Morgan was a book collector and apparently he spent quite some time browsing in Babbage's library, for Tucker's catalogue quotes him for the statement: "*Mr. Babbage's large and rare collection of Tables*". Another name is George Boole to whom, at their first meeting in 1862, Babbage explained the working of the Difference Engine, persuading him to read Menebrea's paper on his Analytical Engine. [45]) However, Babbage may well have been acquainted with Boole's work much earlier, because in his library there was

a copy of Boole's fundamental paper from 1847, *The Mathematical Analysis of Logic*, containing in the margin the note: "*This is the work of a real thinker*". James Joseph Sylvester became interested in Babbage's mechanical notation and, thinking of teaching it, he visited with Babbage for discussion of this and other mathematical topics. Thus, Babbage's library contained donated copies of several of Sylvester's contributions, some of them even autographed by the author. Yet, strangely enough, Babbage did not seem to be acquainted with Sylvester's close friend and collaborator, Arthur Cayley who, after fifteen years at the bar, in 1863 was appointed to the newly created Sadlerian professorship of mathematics at Cambridge.

The controversy between applied and pure mathematics was essentially a question of need and interest. The mathematics carrying Maxwell and the other physicists to success, was more or less created beforehand in its abstract sense. Their emphasis, therefore, had to be on the interpretation in formulation as well as in solution. Contrariwise, the contributions to logic and discrete algebra by De Morgan, Boole, Sylvester, and Cayley, forged the applied tools of our time. Whether driven by aesthetic reasons or the desire to solve problems of a type not yet submitted to a mathematical formulation, no progress was possible under the educational constraint, as Cayley expressed it, "*that pure mathematics should not be studied only with a view to Natural and Physical Science*". [41]) In most of his work, Babbage revealed himself as an applied rather than as a pure mathematician. Still, the lack of appropriate mathematical tools for many of his applications convinced him of the importance of pure analysis. But it appears reasonable to believe that, ultimately, his justification and criterion of success were usefulness. At heart, Babbage was a problem solver.

In this spirit, we shall attempt to uncover a fundamental idea underlying transposition ciphers, and to pin it down as an illustration of a mathematical invariance. However, before that can be done, we first have to solve the problem of the almost elusive boundary between conventional geometry and topology – the question of metric versus non-metric. At the outset, to gain some intuitive insight, let us consider the so-called *skytale*. Developed by the Spartans in Ancient Greece as early as the fifth century B. C., the skytale is a device for military cryptography. Further, it is one of the few apparatus ever devised for transposition ciphers.

According to Lindenfels, [37]) the skytale is formed as a cylindrical staff of wood around which a long and narrow strip of parchment is wrapped closepacked. Always made in pairs of exactly equal dimensions, one for the ephors (or rulers) and one for the commanding general, a skytale was in the order of half a meter in length and about eight centimeters in diameter. The secret message was written down the length of the staff "*on the edges of the strip, where they were joined together,*

such that the letters appeared with one half (e.g. the upper) on one, and with the other half (e.g. the lower) on the other edge of the strip". The parchment was then unwound and sent on its way in this state, where nothing but incomprehensible traces of writing could be perceived. However, when the legitimate receiver rewrapped the parchment on his staff, the separated parts came correctly together making the message readable again

The first to break the skytale cipher appears to have been d'Alembert, who described his technique in the famous *Encyclopédie* on which he worked as co-editor together with Diderot in the years 1746 to 1758. D'Alembert was perhaps even more famous as a philosopher of the Enlightment and for his literary style, than as a physicist. [46]) Thus, since Diderot happened to be imprisoned for a daring public letter, d'Alembert had to undertake the job of giving the program of the *Encyclopédie* in its preface. This was his celebrated *Discours préliminaire*, praised enthusiastically by Voltaire among many others. It may also be mentioned that d'Alembert published a collection of translations from Tacitus, his favourite classical author. Lindenfels, therefore, quoted an authoritative source on the skytale: [47])

> *"This manner of encyphering has always been regarded as insoluble for anyone not possessing such a scytale. The philosopher d'Alembert, however, is of a different opinion. It should not be difficult, says he, by a more careful investigation to find the line which, to make sense in the context, will fit the lower edge of the first line. When first this second line has been determined, it would then be easy to find all of the remainders. Assume that this second line (which according to the context immediately succeeds the first) was, say, the 5th, then all that was needed was simply to pass on to the 9th, then to the 13th, to the 17th, etc., to the end of the strip, and one will thus have found the entire first line of the scytale. From there on, one only needs to consider the second line from the bottom, thereafter the 6th, the 10th, the 14th, and so forth. All this is easy to see, continues d'Alembert, considering that a line written on a roller must be formed by parallel line segments spaced equally apart."*

The point to be emphasized, reading Lindenfels' quotation from d'Alembert, is the almost imperceptible change in argument distinguishing the non-metrical property of topology from the metrical property of Euclidean geometry. The former is merely a question of order: that we have to skip four lines at a time, assuming the lines to be numbered consecutively. The latter is the problem of measuring a distance, assuming equal step in order to correspond to equal step in distance Clearly, the topological viewpoint· the representation of relative position by order, is *more general* than the geometrical viewpoint. In the metrical measure of equal distance is always implied the possibility of ordering. But ordering some objects does not presume anything about distance. Order may be preserved irrespective of

whether or not the objects are spaced equally apart. Hence, in a topological sense quantitative operations, such as taking the mean to find an object in between two given objects, are utterly meaningless. To illustrate, letter *B* in an alphabet is not necessarily half the sum of letters *A* and *C*.

Alexandre-Theophile Vandermonde was the first to recognize the importance of this observation and draw the conclusion that, just as *cardinal* numbers were used as coordinates to describe Euclidean space, so *ordinal* numbers had to be used as coordinates to describe topological space. Music being his first love, Vandermonde turned to mathematics relatively late in life, contributing only four memoirs to the Académie des Sciences in Paris which he entered in 1771. Babbage had acquired two of these papers for his library, the one even with the author's autograph upon it. However, it is the other, entitled *Remarques sur les problèmes de situation* (or remarks on the problems of position), which is of interest to us. Published the same year he entered the Academy, it was concerned with the question of reducing the knight's tour in chess *"to simple arithmetic, using numbers which do not represent quantities at all, but regions of space".* Vandermonde wrote: [48])

> *"I consider space divided into arbitrary finite elements, distinguished by their order; that is to say, (1) I consider a plane divided by parallel lines into a series of strips, and then divided again by another set of parallels which cut the first set; I distinguish the different strips by the designations first, second, third, fourth, etc., in both divisions. I can then describe a given point belonging to any one of the parallelograms formed by the double divisions, by simply writing two numbers, one above the other, where one number is the order of the first division and the other that of the second. Thus, for example, $^4_3$ belongs to the parallelogram which is common to the fourth strip in the first division and the third in the second division. (2) I consider a solid space divided first by parallel planes into a series of slices, then divided again by another series of parallel planes which cut the first ones, and finally divided a third time by a new series of parallel planes which cut both of the others. I can then describe by a symbol 1^2_3, for example, a given point belonging to the parallelepiped common to the third slice in the first division, the second slice in the second division, and the first in the third division"*

In other words, if we compare with APL, Vandermonde writes ^J_I instead of $M[I;J]$ to index an element in a matrix M, and k^J_I instead of $A\ [I;J,K]$ *to index an element* in a 3-dimensional array *A*. Of course, Vandermonde's notation did not invite any extensions to higher-dimensional arrays, but at the time no one thought of going beyond three dimensions. What is, perhaps, more interesting is the fact that Vandermonde's order of the indices is reversed in comparison with the order accepted as standard today and adopted in the APL notation of indexing.

Incidentally, Vandermonde's index notation was not without precedence. Vandermonde was the first to give a connected and logical exposition of the theory of

determinants, so he probably picked up the notation from Gabriel Cramer, the Swiss mathematician and pen-friend of d'Alembert's who, independent of Leibnitz, reinvented determinants in 1750. Thus, in principle, Cramer would write, j^i to indicate the i^{th} row and j^{th} column of a determinant. Therefore, the notation we take for granted, is but an arbitrary choice which posterity found convenient.

Another interesting point in Vandermonde's statement is his notion of a "division" or an *axis*, as we would say today. From his terms "parallelogram" and "parallelepiped", it is evident that he is working with what we would call *oblique* coordinates. Although Fermat, the co-inventor of coordinate geometry together with Descartes, did the same, it is rather unlikely that this would have inspired Vandermonde. I would rather interpret it as an attempt to avoid introducing a metrical measure for the angles between the independent "divisions" or axes. He desired to express the independence following from *rectangularity*, yet had to reject this property as depending upon a metric measure. To escape this dilemma, modern mathematicians have adopted an approach, which we previously have discussed in principle, extending the concept of equilibrium from statics to dynamics.

To begin with, we substitute the rigid, common sense term: "rectangularity" by the technical term: *orthogonality*. Apparently, nothing is accomplished, since this is just a composite Greek word for the same thing. However, the importance of technical terms is that we may assign to them very specific meanings. Therefore, let the term orthogonality imply the condition which in metric space guarantees rectangularity. As is well known, considering two vectors, this condition is that their so-called inner product (scalar product) becomes zero; or, as it is often expressed, their inner product *vanishes*. The notion of orthogonality is now extended from Euclidean space to topological space, carrying this condition of the vanishing product from the metric to the non-metric. By comparison with the extension of the equilibrium concept, the new point here is that we have to introduce a novel kind of inner product, known as the *relative product*. [49]) We shall come back to the relative product later, so let it here suffice to say that it is simply the Boolean counterpart of the conventional inner product.

At present, two things are important. First, the general procedure of extending the validity of a technical notion, focusing on the invariance of some condition which, like the vanishing of a product or sum, is easy to verify in all reference frames. Secondly, the novel conception that topological space is spanned by *orthogonal axes*, without implying any metrical measure at all.

But more can be derived from Vandermonde's description. I am here thinking of the way in which he distinguished between a "plane", characterized by two "divisions", and a "solid space", described by three "divisions". That is, two indices were needed for the "plane"and three for the "solid space". It would seem, there-

1838 Annual Register Chronicle p. 69 *Acc^t of Huberth's campaign against Louis Philip*

Huberth lost his pocket book at Boulogne. It was picked up and opened by the police, was found to contain – "amongst other suspicious papers a letter addressed to M Leproux judge of the court of Verons [?] written entirely in cypher".

"The magistrate charged with the prosecution were for a long time at a loss to produce the key of the cipher in which the letter to M Leproux was written.

"At the end of several months an individual, after studying it for a long time, discovered the secret, and put the Attorney Gen' in possession of its important contents

Every word being represented by two numbers, placed one above the other, this expert suspected that the numbers indicated a reference to some dictionary; that the upper number was the indication of the page, and the inferior on the line where the word was to be found

"All the German, English, and French dictionaries published in Paris were accordingly bought up, and after many a fruitless attempt the expert at last pitched upon the right one and which was the English and French pocket dictionary of Tiby, published by M. Baudry a bookseller living in the Rue de Coq.

"The numbers perfectly adopted themselves to the page and line, and by their means he was enabled to read the very long letter addressed to M. Leproux and two others on which addresses had not yet been written

ndr.

Figure 17. Babbage's note illustrating a book cipher. (BL, Add Ms. 37205, FF. 32-33)

fore, that the number of indices needed for the description would define the dimensionality of the topological space. Although a natural conclusion to draw from the experience with Euclidean space, it was discovered by Henri Poincaré and other mathematicians at the turn of our century, that it does not hold in general For a while, however, let us neglect this problem in order to obtain some intuitive understanding of the notion of topological dimensionality.

A good illustration to bring across this non-metrical idea, is the *book cipher*. Babbage's note on Huberth's cipher, transcribed in figure 17, provides a simple example based on the use of a dictionary. In an abstract sense, this dictionary is but a physical representation of Vandermonde's topological "plane". Each word in the dictionary corresponds to a point in the plane. The pages and the lines make up the two "divisions". To find the relative position of a word in the dictionary is tantamount to finding the relative position of a point in the plane. The page number and the line number are the two ordinal coordinates needed, and, as Vandermonde's indices they are "*placed one above the other*".

A disadvantage inherent in the use of dictionaries, is that the same word is always represented by the same pair of indices. Also, a message might contain words (e.g. names) which cannot be found in the dictionary. Further, as evident from Babb-

age's example, dictionaries may be traced. To permit the use of books in general, one has to increase, therefore, the number of indices. An initial step in this direction is to introduce a third index in order to identify the word number in the line. Thus, according to Lindenfels, the index notation: i^j_k would mean page *i*, line *j*, and word *k*. Apart from the reversal of index order, this clearly corresponds to Vandermonde's indexing of his "solid space". Hence, this type of book cipher may be conceived as a 3-dimensional topological space.

However, to permit spelling of words, Lindenfels recounts that further indices may be added, identifying either the letter number or the syllable number in the word. In fact, he even describes the addition of a pair of indices which in the given word identifies the syllable number and, within the syllable, the letter number.

Rather unwieldy in practice, the latter construction is of interest from a mathematical point of view. To identify the relative position of a letter, five indices are used: $i^{j\,l}_{k\,m}$ meaning page *i*, line *j*, word *k* and, within this word, syllable *l* and, within this syllable, letter *m*. Yet, we would only conceive this book cipher as a 3-dimensional topological space (identified by page, line, and word), since the last two indices (syllable and letter) describe a *nesting* within the word and the syllable, respectively. In other words, the notion from Euclidean geometry that the number of indices determine the number of spatial dimensions, has broken down for topological spaces. This is about as close as we can get with a non-technical explanation of the findings of Poincaré and others.

Vandermonde, as we recall, was concerned with the problem of the Knight's tour in chess. His topological objects, the "plane" and the "solid space", were therefore basically finite in conception. Hence, in modern terminology we may conceive them as tabular arrays of two and three dimensions, respectively. The book ciphers are also finite, but considered as arrays they fall into two distinct classes. On one hand, we have 2- or 3-dimensional tabular arrays determined by the pair of indices: [page, line] or the triple of indices: [page, line, word], respectively. On the other, we have nested arrays using the additional indices: [syllable] and [letter] to index one or two levels down in the topological structure. That is, the nested array is characterized by the fact that its elements are again arrays, and so forth. For example, the "word" is a list (1-dimensional array) of "syllables", each of which is again a list of "letters".

In this geometrical description, three things are of central importance to our general understanding of arrays as topological objects. Basically, they are: the *assumption of finiteness*, the abstract notion of *order as a binding topological property*, and the aspect of *empirical interpretation*. Let us take a closer look at each of them.

The question of infinity is a basic cause of complication in most branches of mathematics. Accordingly, the assumption of finite arrays is a very strong and most

significant simplification. Technically, a *finite array* is characterized by a finite number of orthogonal axes, each of which is extended finitely. That is, each axis is specified by a finite number of indices or ordinal coordinates. Because of this assumption, it is natural to describe an array as a geometrical or topological object. However, in a geometrical sense it is often more advantageous to conceive an array as a *finite topological space;* a limiting case, so to speak, of our conception of infinite geometrical spaces or *manifolds*, as it was termed originally by Herman Günther Grassmann, and popularized by Georg Bernhard Riemann, to get away from the conventional Euclidean notion of a 3-dimensional space.

Grassmann proposed the concept in 1844 in his book *Die lineale Ausdehnungslehre* (Calculus of Extension) which title, according to Felix Klein, is an abbreviation of "*die Lehre von ausgedehnten Mannigfaltigkeiten*" (a theory of extended manifolds). It is in this work that we find introduced "*the conception that an element of an arbitrarily extended manifold may be considered analogous to a point of conventional space*". 30) Of course, no explicit meaning needs to be assigned to the undefined concept of a point. As David Hilbert, the leading mathematician at the beginning of our century, once put it: Anyone is at liberty to replace points, lines, and planes by tables, chairs, and beer mugs. However, it is intuitively suggestive to consider a manifold of *n* dimensions as the spatial aggregation of a set of points, just as the aggregate of the points on a surface in Euclidean space constitutes the surface itself. The points of such a manifold are in one-to-one correspondence with *n-tuples* of variable parameters: $(x_1, x_2, \ldots x_n)$, the *coordinates* of the manifold, but, in general, concepts such as length, angle, area, parallel displacement, and curvature are completely missing. What distinguishes a manifold from a mere point set is some basic property binding the points together, just as distance between points in Euclidean space tells us how close to each other the points are. The binding property, turning the point set into a space, may be termed the *connectivity* of the manifold. Being open to any definition, this concept is basic to the classification of manifolds.

It is evident from this description that the notion of an array, whether tabular or nested, may be interpreted geometrically as a *finite manifold*, now calling the point a *datum* (plural: *data*), provided that we can give the binding property of the set of data an appropriate definition. Clearly, a basic requirement to such a definition must be that our intuitive notion of a *data structure* finds its mathematical expression as a concept we can identify with the connectivity of an array. As we shall now see, this leads us to the introduction of order as the binding property of fundamental importance.

In Euclidean geometry, it is well known that many a "proof" can be given of false results, because Euclid's axioms do not dictate the location of certain points in relation to others. 22) The first to discover that Euclid tacitly used properties of

order without having stated them as axioms, was Moritz Pasch who gave, in his *Vorlesungen über neuere Geometrie* (Lectures on Modern Geometry) from 1882, a set of axioms for the order of points on a line, the so-called *concept of betweenness*. However, it was David Hilbert's *Grundlagen der Geometrie* (Foundation of Geometry), published 1899, which supplied today's favourite revision of Euclid's set of axioms. The flavour of this extension may be illustrated by one of his axioms of betweenness: *"If a point B lies between points A and C, then A, B, and C are three different points on one line and B also lies between C and A"*

The important point here, is that such *axioms of order* must also be incorporated in a complete set for any one of the metric geometries. This explains that when all metrical properties are removed from geometry, order is preserved as a fundamental non-metric property. In particular, since it is possible to set up the different kinds of geometry from the unified standpoint of general set theory, partial order as exemplified by the well-known operation of *set inclusion*, will be such a non-metric property. However, a basic disadvantage of this operation, from our point of view, is that it admits incomparable elements. What we desire, is another principle which eventually will permit us to establish a total order. It is for this reason that the assumption of finiteness becomes of critical importance.

The essence of this assumption is that the array may now be conceived as a so-called *countable set*, in the sense that its data or elements are denumerable. This implies, that a one-to-one correspondence may be established between the data of the array and a set of ordinal numbers. Since the latter set is totally ordered, so the data of the array will submit to a total ordering. Georg Cantor, the founder of set theory, recognized that the property of basic importance is not total order as such, but the fact that every set of ordinal numbers has a smallest element. He therefore introduced the abstract notion of a *well-ordered set*, meaning that every non-empty subset has a first element. Clearly, in this form we have a local principle, the repeated application of which may be used to derive total order. In a geometrical sense, well-ordering may be introduced like distance to describe the connectivity of a manifold. Thus, it is for good reason that well-ordering defines the binding property of the finite manifolds known as arrays. [51])

Apart from a few cursory remarks later on, we shall not go into any detail on the question of nested arrays. All that we need to know, is that well-ordering is as fundamental to nested arrays as it is to tabular. In fact, based on this definition of connectivity it is possible to derive the concept of tabular arrays as a special case of that of nested arrays. [52]) But let us now turn from the abstract geometrical notion of arrays to the associated aspect of the empirical interpretation.

Undoubtedly, the most obvious advantage accruing from the geometrical representation of data, is the intuitive relation it has with direct experience. In Euclidean

geometry, many theorems were discovered as the result of experiments with ruler and compass or similar instruments. Likewise, many of the abstract properties of arrays have their inspiration in practical applications. Most conspicuous in this respect, perhaps, is the distinct difference in interpretation between, what we here have called, the data and the data structure.

Measurements, in the most general sense of the word, constitute the only link between the observations of reality and our corresponding abstract conception or theoretical model hereof. Colloquially, the concepts of measurement and data are almost synonymous. Both terms are used to denote the recorded representation, say the colour "red" or the weight "30 kg", of the act of measuring or of the derived consequences of this act. Under closer scrutiny, however, we discover that in the notion of measurement is implied an additional content, depending upon the actual act of measuring. To make a measurement meaningful and open to verification, it is not enough to give the observed "value" of the property in question. We must also identify, among other things, the object or the event possessing this property. A little reflection will show that, normally, it is this additional and context-dependent identification that is captured in the associated data structure. Further, what makes it a structure is the fact that we relate the specific object or event to the other objects or events forming the real-life system under consideration.

The fact that a datum is associated with a property and a data structure with a system of things possessing this property, explains that one and the same data set may be represented in terms of alternative data structures. For example, instead of considering the dictionary book cipher as a table, indexed by the coordinate pair [page, line], we might focus on the look-up procedure and represent it as a nested list of lists. That is, a list of pages, each page of which is in turn a list of lines. Incidentally, this arbitrary choice of data structure illustrates that, basically, tabular and nested arrays are governed by the same principle of order.

2.7 According to Professor Petersen

The geometrical conception of data is in the main stream of scientific development. Rooted in the common experience of physical space, it has a long and venerable tradition in mathematics. In practical applications, incorporating the complexity in the formulation of the data structures, it provides for powerful operations clothed in simple syntax.

As in other walks of life, however, the degree of insight and understanding is a limiting factor. The most serious barrier in this respect, seems to be encountered in those situations when the mathematics go beyond basic experience and intuition

The notion that the axes of an array are but an ordering device, illustrates the problem. Our conception of space is imbued with metric measures, almost independent of the level of abstraction. Whether a transformation from Cartesian to polar coordinates, or the affine mapping of descriptive geometry for drawing a perspective, our thoughts are governed by the image of physical space. We find it difficult to take advantage of the flexibility inherent in the non-metric view.

Fractionating or *tomographic* ciphers constitute a class of systems which, based on a 2- or 3-dimensional coordinate representation of the letters, severs the axes of coordinates from one another. Hence, the use of the Greek word *tomos*, meaning a cut or a section. In the 2-dimensional case, the substitution of each plaintext letter by an ordinal coordinate pair is usually accomplished by some kind of checkerboard satisfying the condition that each and everyone of its positions corresponds to a distinct letter or other symbol.

Pliny Earle Chase, a professor of mathematical sciences at Haverford College near Philadelphia, apparently published the first description of such a cipher in 1859 in the new *Mathematical Monthly*. His approach, as described by Kahn, was based on a checkerboard substitution the coordinate pairs of which were split into two separate lists of row and column indices, respectively. The letter order of the plaintext was preserved in both lists, and the column indices were transformed by some substituting technique, such as adding a repeating key, and then paired again with the row indices. By use of the checkerboard once more to interpret the list of revised coordinate pairs, a cryptogram of enciphered letters was produced. Although far superior to many of the systems in use at the time, the invention passed unnoticed.

Sixteen years later, the basic principle of separating the coordinate pairs of a checkerboard was rediscovered by another mathematician. Unaware of Chase's contribution, he let his invention take a different direction submitting the coordinates to various transposition techniques. Before we go into more detail on his cipher, however, a brief sketch of the inventor will be in order. [53])

Born in 1839, Peter Christian Julius Petersen, later in life signing himself merely as Julius Petersen, in 1860 passed the undergraduate study at the Technical University of Denmark with honours, before he discovered that mathematics was his vocation. He therefore continued his studies at Copenhagen University, winning the Gold medal of 1867 for a thesis on the equilibrium of floating bodies. Obtaining his doctoral degree in 1871 for another thesis on equations solved by square roots, he was appointed associate professor at the Technical University the same year. From 1881, he served simultaneously as teacher of mathematics at the Royal Military Academy. In 1887, he gave up these two position for a new chair in mathematics at Copenhagen University. He died in 1910.

An important figure in Danish mathematics, he was a member of the board of inspectors of senior schools (1887-1900) and was nationally known as the author of a series of school and undergraduate textbooks, one of which, *Methoder og Theorier til Løsning af geometriske Konstruktionsopgaver* (Methods and Theories for the Solution of Problems of Geometrical Construction), published 1866, achieved international recognition being translated into seven languages (German, French, English, Italian, Hungarian, Russian, and Dutch). This basic concern for geometry led him to an interest in algebraic invariants and group theory which in 1877 resulted in a brilliant new book, *De algebraiske Ligningers Theori* (The Theory of Algebraic Equations). This work, about which I have more to say later on, was translated into German, French, and Italian.

Corresponding with Sylvester, in particular, he was inspired to carry his research into topology, resulting in 1891 in the publication in Acta Mathematica of his most famous paper, entitled *Die Theorie der regulären Graphs*. The influence of British mathematics is felt in the strange syntax mixing the English word "graph" into a German context. Hailed today as "*a landmark in graph theory*", [48]) this paper was so far ahead of its time that Dénes König wrote in 1936, in the first book on graph theory: "*This thesis by Petersen, to which also Sylvester has contributed, is doubtless the most important work in graph theory, though it has been completely ignored for more than 25 years*". It is interesting to note in this connection that some of the tools forged by Petersen in this paper, only now, about a century later, find their way into modern control theory. [54])

Hieronymus Georg Zeuthen, Petersen's close colleague holding the other chair in mathematics, described him admiringly as a renaissance figure who, with uncanny geometrical intuition and without bothering too much about the existing literature, excelled in solving all kinds of problems in the most original, simple, and natural manner. The intensity with which he worked was most peculiar, and as long as he was occupied by a problem, he would return to it again and again in his discussions. Fortunately, Zeuthen adds dryly, Petersen had some understanding friends.

The result of one of these multi-varied interests was a 15 pages pamphlet in French, *Système Cryptographique*, printed privately in November 1875. [55]) Since Petersen contributed to a variety of professional journals, it seems reasonable to assume that he intended this publication for a select clientelle only.

By way of introduction, Petersen explains that although a multitude of cryptographical devices and a rather voluminous literature have grown out of the ever existing need to make secret communications, the problem has not yet found a satisfactory solution; and he continues:

"The author of this note, having done some research on the most well-known systems, has demonstrated that none of them can resist the efforts of an able decipherer. This is the case for the "Carré Indéchiffrable" [i.e. the Vigenère], *the system of Mr. Willard, and that of Mr. Léopold Auvray (Nouvelle Cryptographie, Paris 1870), where the periodicity facilitates the solution whenever the dispatch is about twenty times longer than the key. Mr. Wheatstone's cryptograph is a handsome apparatus which offers a great measure of security, and the same applies to the novel devices of Messrs. Orloff and Sommerfeldt. Yet, without knowing the key, I have succeeded in deciphering dispatches written according to these systems. This year has seen a pretty discovery by Mr. Flamm (this method, by the way, is not new. See Kluber: Kryptographik, 1809), but even if it is operated on far more easily than all its predecessors, it leaves much to be desired with respect to security".*

All of these names, apart from that of Wheatstone, have long ago sunk into oblivion. J. L. Kluber (whom Petersen misspells as Klüver) has survived in Lindenfels' account where it is demonstrated beyond doubt, notwithstanding Kluber's euphoriant claims to the opposite, that Vigenère's classical cipher has been reinvented once more. Among the remaining names, only two catch the eye; namely, those of Orloff and Sommerfeldt, because the earliest known Danish Army manuals for cryptographical devices are one from 1873 describing Count Orloff's apparatus, and another from 1883 explaining Captain Sommerfeldt's system. Placed in between these two dates, Petersen's invention may well have been offered to the Danish Army, even though a diligent search in the army archives was negative in this respect. [30] Neither did the search bring anything to light indicating that the cipher was ever taught to or used by Danish military personnel. Whether Petersen had more success elsewhere, is not known.

In his introduction, Petersen also describes the basic requirements, with respect to security as well as facility in use, which must be met by the inventor of a cipher. Apart from more obvious specifications, such as simple and speedy character manipulations, he has also some of no little insight. For example, that the system should be self-correcting, since errors are unavoidable in the telegraphic transmission. Or, that the security of the system should be measured against the fact that the "enemy", knowing the system, has at his disposal a large number of dispatches enciphered with the same key. Indeed, he suggests as a practical test of his own system that all dispatches but one in this set should also be given in plaintext.

Regarding a theoretical analysis of a cipher, he says that one should be aware that different linguistic combinations are of different probabilities. Hence, he continues, the usual claims based on some larger number of combinations signify nothing, because they assume them all to be of equal probability:

"It is the task of the decipherer to find the combinations of great probability. Normally, this requires a man who is a trained decipherer and an able mathematician. In a manner of speaking, this does not mean that knowledge of mathematics is necessary, but rather that he must be imbued with that particular kind of acuteness which is developed especially in the study of the mathematical science."

But let us turn to Petersen's description of his cipher, postponing a detailed illustration of its use to the APL terminal session at the end of part two.

A prerequisite for the use of the cipher, is a square checkerboard alphabet. To exemplify how this is established, Petersen considers the case of a 25-letter alphabet (dropping letter W). Arranged in a 5-by-5 square, it is randomized

\	3	1	4	5	2
5	A	B	C	D	E
2	F	G	H	I	J
1	K	L	M	N	O
4	P	Q	R	S	T
3	U	V	X	Y	Z

=>

\	1	2	3	4	5
1	L	O	K	M	N
2	G	J	F	H	I
3	V	Z	U	X	Y
4	Q	T	P	R	S
5	B	E	A	C	D

permuting the row and the column indices according to some numerical double-key:

KEY1: ROW←5 2 1 4 3 & COL←3 1 4 5 2

According to his description, the left-hand table will suffice, both for the substituting of a letter by a pair of indices and for the opposite substitution. Still, the rearrangement shown in the right-hand table may be more convenient for the latter purpose.

With the checkerboard thus established, Petersen turns to the problem of how to encipher messages. Since he intends to accomplish this by a *double transposition* applied to a rectangle, he begins by introducing an assumption on the size of the plaintext message. Namely, that adjusted by dummy letters, the so-called *nulls*, its number of letters is that of the number of positions in a rectangle of 10 rows and an arbitrary number of columns. To illustrate, he gives a 98-letter message: *"Le problème de déterminer combien il y a de nombres premiers compris entre deux nombres donnés n'est pas encore résolu"* (the problem of determining how many prime numbers there are between two given numbers, is not yet solved). Adding the double letter *"qq"*, playing the role of nulls, to the end of this message, he adjusts it to the size of a 10-by-10 rectangle of letters.

The next step after this adjustment of size, is the substitution of each letter by its corresponding pair of indices. Using the checkerboard and neglecting accents, punctuations, and spaces, he finds:

L	E	P	R	O	B	L	E	M	E
(11),	(52),	(43),	(44),	(12),	(51),	(11),	(52),	(14),	(52),

which nested list of one-hundred pairs he transforms into a tabular list of two-hundred 1-digit integers.

1 1 5 2 4 3 4 4 1 2 5 1 1 1 5 2 1 4 5 2 ...

Conceptually, this fractionating of the indices is a step of utmost significance. By destroying the basic difference between 1st coordinate and 2nd coordinate it reveals that the two axes of the checkerboard constitute but an ordering device. Because of the lack of metric measures, the checkerboard does not possess the intrinsic properties of dimensionality commonly associated with our conventional notion of space. Hence, the representation by a square table is merely a convenient geometrical image.

The tabular list of two-hundred indices is now rearranged by a *diagonal* route transposition, based on a 10-row rectangle. Since the number of columns depends on the length of the message to be conveyed, his example evidently requires 20 columns. Adopting the so-called *ascending* diagonals, *"like the bishop in chess"*, he obtains:

	1	2	3	4	5	...
1	1	5	3	2	5	
2	1	4	1	1	2	
3	2	4	1	5		
4	4	1	4			
5	5	1				
6	2					
⋮						

by the route

	1	2	3	4	5	...
1	1	3	6	10	15	
2	2	5	9	14	20	
3	4	8	13	19		
4	7	12	18			
5	11	17				
6	16					
⋮						

To destroy the diagonal pattern this rectangle is further submitted to a *columnar* transposition, based on a permutation of the column indices according to set a numerical key, say

KEY2←7 3 5 9 14 10 2 12 6 1 8 13 4 11 17 15 16 18 20 19

Thus, he finds.

	7	3	5	9	14
1	1	5	3	2	5
2	1	4	1	1	2
3	2	4	1	5	
4	4	1	4		
5	5	1			
6	2				
⋮					

=>

	1	2	3	4	5	6
1	5	2	5	4	3	5
2	5	1	4	5	1	5
3	1	4	4	1	1	3
4	2	1	1	5	4	5
5	1	1	1	4		
6	5	2				

Joining the columns two and two to form pairs of indices, he obtains a revised rectangle of only half the number of columns (here 10)

	1	2	3
1	52	54	35
2	51	45	15
3	14	41	13
4	21	15	45
5	11	14	
6	52		
⋮			

By going down the columns, beginning with the leftmost, we obtain a transformation of the rectangle into a nested list of coordinate pairs:

(52), (51), (14), (21), (11), (52),

By use of the checkerboard once more, this list is substituted by letters, blocked into groups of five:

EBMGL ERCCH CSQNM

This forms the enciphered message, ready to be dispatched.

Depending on the size of the message, we may have to add from 1 to 9 dummy letters or nulls. To cut this number down to 4 at most, Petersen suggests that the diagonal route transposition be extended to rectangles of an odd number of columns whenever appropriate. Since the pairing of indices after the two transpositions is based on an even number of columns, Petersen introduces the additional rule *"If the number of columns is odd one takes the indices of the last, two by two from top to bottom"*

As I have presented it here, two keys: KEY1 and KEY2, are needed. In actual fact, however, Petersen derives both keys from one and the same keyword or key-sentence, recommending a total length of about 15 letters. Apparently, this dual role is reflected in the wording of his illustrative 14-letter key: "*Le jour et la nuit*" (the day and the night). The difference between the derived keys is determined solely by the sequence of letters selected from the common keyword. From there on, the same principle governs the substitution of letters by numerical indices. The basic idea is to assign each letter of the derived sequence the index of the position it would have had, were the sequence ordered alphabetically. Yet, since repeated letters are mutually ordered from right to left, the operation does not entirely coincide with the *grade up* operation in APL.

To create the double-key: KEY1 for the checkerboard, all vowels are removed from the common keyword. The row indices: ROW, are then derived from the last 5 consonants (taken from right to left), whereas the column indices: COL, are produced from the first 5 consonants (in their usual order):

$$\text{ROW} \leftarrow \text{T N L T R} \quad \text{and} \quad \text{COL} \leftarrow \text{L J R T L}$$

Applying the revised "grade up" rule, we find the two lists of indices given previously.

The key: KEY2 for the columnar transposition, requires a repetition of the keyword to match the twenty columns of the rectangle of indices:

$$\text{KEY2} \leftarrow \text{L E J O U R E T L A N U I T L E J O U R}$$

However, instead of applying the revised grade up rule directly to this entire sequence, Petersen applies it to the initial 14 columns (determined by the original keyword) separately from its application to the final 6 columns (determined by the key extension). This explains how the list of column indices was obtained. Although not stated explicitly, Petersen's approach would seem to suggest that the permutations of the initial 14 columns should be prepared once and for all simultaneously by means of the checkerboard. Another feature to save work and diminish the number of errors, briefly mentioned by Petersen, is an apparatus with movable slips for performing the columnar transposition. Such an apparatus, he claims, could be made quite handy to fit a pocket book.

Petersen concludes his description of the encipherment process by saying that the decipherment is accomplished by performing the operations in inverse order. After having tried these processes two or three times, one should be able to encipher (decipher) a dispatch of one hundred letters in about 12 minutes or, if the apparatus is used, in 8 minutes. For trained army personnel, 5 minutes should suffice.

Concerning the problem of a cipher letter garbled in the telegraphic transmission, Petersen points out that in the plaintext this will affect only the first coordinate of one letter and the second coordinate of another. Hence, to correct the error one should enter a row and a column of the checkerboard in search of the two letters most probable in the context. Petersen also remarks that, although the checkerboard may be increased in size to a higher square number, it is most convenient to retain the 25 letters. Numbers, rare letters, countries, and the like, may be expressed by the same checkerboard, giving the 25 letters additional interpretations signalled by *index* or *changer* signs in the form of preceeding letters agreed upon.

While teaching at the Royal Military Academy, Petersen may have discussed his ciphers with various officers. He may even have demonstrated it to the cadets in class However, like so many other novel ciphers, it made no impact at the time.

The first, therefore, to gain recognition for the invention of a fractionating system based on transposition of the coordinates, was Félix Marie Delastelle who, twenty-seven years later, in 1902, published such a cipher in his book: *Traité Élémentaire de Cryptographie*. This was the so-called *bifid*, a cipher of considerable importance to the development of cryptography. [57]) Although we shall refrain from going into any detail on Delastelle's contribution, it may be mentioned that in a cipher, known as the *trifid*, he generalized this idea to a 3-dimensional "checkerbox" alphabet, in which each of the 27 letters (adding *é* in French, or & in English) are identified by a triple of coordinates. In the literature, the latter alphabet is known as the *Trithemius alphabet* after its inventor, a Benedictine abbot, Johannes Trithemius (1462-1516), the author of the first printed book on cryptography.

2.8 Pinning Down an Invariant

It is common experience that a lump of clay or dough may be hammered flat, or even rolled into a long string. Although the shape is changed from 3 dimensions to 2 dimensions, or even 1, we do not hesitate to say that it is the same lump. By weighing it in its different shapes, we can convince ourselves that it contains the same number of particles.

We find no difficulty in generalizing this physical picture to the abstract notion of a tabular array. Such an array, like the lump of physical matter, may be reshaped from a 3-dimensional box to a 2-dimensional table or even a 1-dimensional list. Independent of the number of dimensions, the shape will be of finite extension. So we can always verify by counting, that the array, whatever its shape, will consist of the same number of "cells" or points

The reason why we find this idealization intuitively satisfactory, is that we perceive the array to be a kind of elastic thing. Stretching, bending, flattening, or

rolling, are but topological transformations of one and the same geometrical object – the array.

Earlier, however, we introduced an alternative interpretation of an array, conceiving it as an abstract type of geometrical space called a finite manifold. Invoking this point of view, we are forced to accept that dimensionality in the conventional Euclidean sense is no inherent property of spaces. In connection with the discussion of the book cipher, we illustrated the breakdown of the traditional notion that, if n coordinates were needed to specify a point, the space had to be n-dimensional. But even then, the whole idea is so strange, so contrary to physical experience, that at least subconsciously we wish to reject it. As we ponder the problem, it might occur to us that perhaps we fool ourselves: Is the notion of a "finite space" but another term for a "geometrical object"? Or, is it truly a special case of the general conception of infinite spaces of different dimensions? To resolve this question is clearly of vital importance. Without this insight, we would find it difficult to pin down the invariant property characterizing an array as its shape is changed from one number of dimensions to another.

If we return for a minute to our picture of the lump of physical matter, most of us would intuitively accept that, steadily increasing the amount of matter, we could fill up the points of a line faster than those of a plane and, in turn, the points of a plane faster than those of conventional space. The reason why we feel this to be true, is that all physical experience seems to indicate, that the number of points on a line is less than the number of points on a plane, which, in turn, is less than the number of points in space. In the face of infinity, however, physical experience falls short. Whether an infinite line, an infinite plane, or an infinite space, the number of points is the same. But since this property is basic to the different shapes of an array, we begin to understand why an array is a special case of an infinite manifold.

The first to attempt a comparison of two infinite entities, was Galileo Galilei. After his trial before the Roman Inquisition in 1633, he was placed into a kind of house arrest and forbidden to publish. Nevertheless, he undertook to write up his years of thought and work on the phenomena of motion and of the strength of materials. Secretly transported to Holland, the manuscript was published there in 1638. Entitled *Discourses and Mathematical Demonstrations Concerning two New Sciences*, usually referred to today as *Dialogues Concerning Two New Sciences*, this was the classic in which Galilei presented his new scientific method. In it, he also broke new ground in mathematics, establishing a one-to-one correspondence between an infinite set and a proper subset. 58) Thus, he assigned the set of natural numbers: 1, 2, 3, ... to its subset of square numbers: 1, 4, 9, ... as follows:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1 & 4 & 9 & 16 & 25 \ldots \end{array}$$

Common sense dictates that the upper row contains "more" numbers than the lower. Still, by this assignment Galilei comes to the conclusion that concepts such as "larger" or "smaller" cease to be applicable. All one can say, is that both sets are infinite.

Galilei's view, that infinity cannot be graded according to size, came to dominate mathematical thinking. Gauss, in a letter to Schumacher of July 12, 1831, said: *"I protest against the use of an infinite quantity as an actual entity; this is never allowed in mathematics. The infinite is only a manner of speaking ..."*. Indeed, as late as 1909, he was seconded by Poincaré, that what we call infinite is *"merely the possibility of continually constructing new objects, no matter how many have already been constructed"*. From this viewpoint, therefore, our statement that an infinite line, an infinite plane, and an infinite space contain the same infinity of points, is meaningless; except, of course, as a manner of speaking.

Georg Ferdinand Ludwig Philipp Cantor, the creator of modern set theory, thought differently about the matter. He dared, as in 1883 he wrote in a paper, *"putting myself in opposition to widespread views regarding infinity in mathematics and to current opinions on the nature of number"*. Schooled in Plato, Aristotle, and the medieval scholastics, he believed that infinity existed *"in actu"* as a measure of totalities or a concrete entity, the *actual infinite*, to be seen in contradistinction to the prevailing notion of the *potential infinite*, the latent possibility of forever creating or adding one more item. Considering that the actual infinite had been an inadmissible concept to mathematics since Aristotle in his *Physics* concluded, *"The alternative then remains that the infinite has a potential existence ... There will not be an actual infinite"*, this was a bold step. Still, incredible as it may seem today, in a correspondence with Cardinal Franzelin, Cantor defended his view by reference to the classical attempts in theology at "proving" God's existence. 58)

Following Thomas Aquinas, this is done by demonstrating that there must be an ultimate cause of everything, namely God. In principle, such a "proof" proceeds by infinite recursion, explaining the cause of one effect as the effect of a previous cause, etc., yet ending up with an "ultimate cause". Adopting a modern terminology, we could say that Cantor interpreted the invoking of such a stop criterion for an infinite loop as the establishment of a measure of infinity. For theological reasons, therefore, he felt that the concept of actual infinity had to be accepted in mathematics.

Where Babbage had a rather relaxed relationship to Greek philosophy, as indicated by the sham quotation on the title page of his *Passages* (see figure 2), Cantor was deadly serious. Thus, in a note to his mathematical definition of a set, Cantor explicitly remarked that he believed here to have captured the fundamental concept discussed by Plato in his dialogue *Philebus*. [56]) It is thought-provoking in this connection that, where Richard Dedekind, his close mathematical friend, perceived a set as an aggregation of things, Cantor once described it as an "*abyss*"

But Cantor was also influenced in a more general sense by the philosophy of Plato. This philosophy stresses especially that actual things are copies of transcendent ideas and that these ideas are the abstracts of true knowledge apprehended by reminiscence. Counting mathematics among the actual things, Cantor looked upon this discipline as a sort of auxiliary science to metaphysics. Thus, in a letter of February 2, 1896, to Father Thomas Esser in Rome, he wrote: [58])

> "*The establishing of the principles of mathematics and the natural sciences is the responsibility of metaphysics ..... The general theory of sets, which you will find in the paper 'On the lore of transfinite numbers', as well as in the first paper of the work* Contributions to the Foundations of Transfinite Set Theory, *which I have begun, belongs entirely to metaphysics. You can easily convince yourself of this by testing the categories of cardinal number and ordinal type, these fundamental concepts of set theory, with respect to the degree of their generality, and also notice that the reasoning about them is quite pure, so that fancy has no room to play*
>
> *This is in no way changed by the pictures which I, like all metaphysicians, sometimes make use of to explain metaphysical concepts. Nor does the fact that my work appears in mathematical journals affect its metaphysical character and content*".

Undoubtedly, this belief inspired him to go against the accepted view of the mathematical society. It also substained him in the face of adversities, ridicule, and even personal attacks which, at one point in time, even drove him into a nervous breakdown His ideas on transfinite ordinal and cardinal numbers aroused the outright hostility of Leopold Kronecker, the powerful number theorist in Berlin, who attacked them savagely over more than a decade. Felix Klein was by no means in sympathy with his approach. Poincaré referred critically to his set theory as an interesting "*pathological case*", predicting that later generations will regard it "*as a disease from which one has recovered*". Hermann Weyl spoke of his notational hierarchy of alephs (the Jewish letter: A) as "*a fog on fog*" [illegible])

Gradually, however, more and more prominent mathematicians were won over to his view, impressed by the uses to which the new theory had already been put. Hilbert spread his ideas in Germany, and in 1926 said: "*No one shall expel us from the paradise which Cantor created for us*". He praised Cantor's transfinite arithmetic as

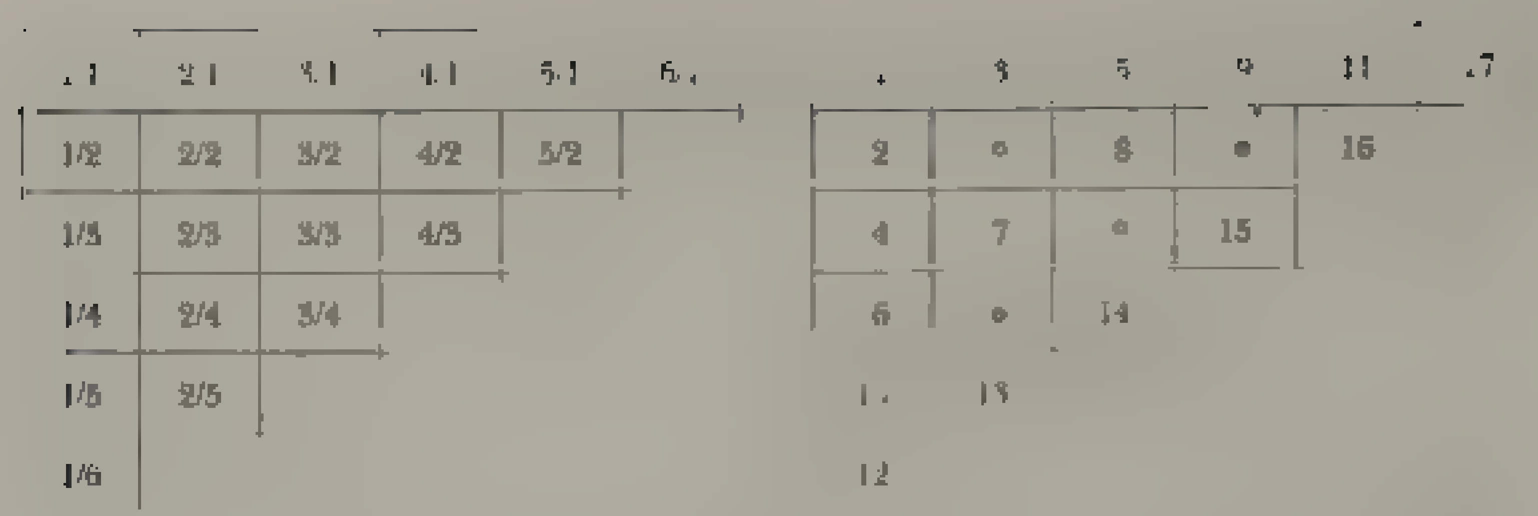
"*the most astonishing product of mathematical thought, one of the most beautiful realizations of human activity in the domain of the purely intelligible*". Bertrand Russell described Cantor's work as "*probably the greatest of which the age can boast*" [22])

Among Cantor's friends and admirers was a Berlin gymnasium teacher, F. Goldscheider. On one occasion he asked Cantor, then professor in Halle, several questions about the latter's theory of sets. In a delightful letter of June 18, 1886, published for the first time some twenty years ago, [59]) Cantor answered with a completeness almost turning the letter into a small handwritten textbook on the fundamental ideas of set theory up to the notion of well-ordering

To convey the basic ideas in an intuitively simple manner, Cantor gave a wealth of examples in this letter. Among his illustrations of the concept of well-ordering, we shall consider an example concerning the positive rational numbers. Geometrically, this set of numbers originates in the fact that a line-segment can be doubled, trebled, etc., but also that it can be halved, divided into three, etc. Starting with the unit segment, we obtain segments of the length m/n in this way, where m and n are natural numbers. These segments correspond to the positive rational numbers (i.e., fractions such as $4/5$ or $3/2$);. On this basis, according to Cantor, a possible well-ordered set is

> "*The set of all positive rational numbers arranged in the following order:*
>
> $(1/1, 1/2, 2/1, 1/3, 3/1, 1/4, 2/3, 3/2, 4/1, 1/5, 5/1, 1/6, 2/5, 3/4, 4/3, 5/2, 6/1, \ldots)$
>
> *The rule for ordering here is that of two positive rational numbers* m/n *and* m'/n' *in* reduced *form* [that is, in lowest terms], *the first has a* lower *or* higher *rank than the second according as* $m+n$ *is smaller or larger than* $m'+n'$; *however, if* $m+n = m'+n'$, *the ranks depend on the relative sizes of* m *and* m'. *In* this *ordering, every non-empty subset has a first element. With the usual order relation* ($a<b$) *this is not the case: the set of all rational numbers of the form* $1/n$ *has no smallest element*".

It is well known that geometry was a constant source of inspiration to Cantor Consequently, we may assume, corresponding to Vandermonde's approach or the simple book cipher, that he conceived the fraction m/n as a pair of indices, specifying the position of the fraction in a table on infinite extension along its rows and columns. Figure 18A illustrates the formation of such a table with the columns given by the numerators and the rows by the denominators. It is evident that this table will contain the set of all rational numbers. Of course, some of these numbers are repeated, as the duplication ($1/1$, $2/2$, $3/3$, ...) in the main diagonal from upper left towards lower right, but the superfluous entries can always be removed at a later stage.



A) Well-ordered set of all positive rational numbers *B) Assignment of the integers*

Figure 18. Reconstruction of Cantor's approach from his letter of June 18, 1886, to F. Goldscheider.

Considering the ascending diagonals from lower left to upper right, as in Julius Petersen's cipher, we notice that the sum of the numerator and the denominator is constant over a given diagonal. Further, the ascent along such a diagonal, is characterized by a steady increase in value of the numerator. Clearly, Cantor's rule for ordering is derived by consideration of these two properties of the diagonals.

Hence, beginning in the upper left corner and proceeding along one ascending diagonal after the other, we can establish a one-to-one correspondence with the natural numbers. Since in this process any fraction, which can be reduced to lower terms, must be a duplicate of a fraction encountered earlier, we even have a fixed rule for eliminating duplicates. Figure 18B shows how, by invoking this latter rule, the sequence of positive integers is assigned to the positions of all fractions on non-reducible form, skipping all positions corresponding to fractions on reducible form.

Basically, Cantor's ordering of the rational numbers in this table, is but the establishment of an infinite route transposition providing a one-to-one correspondence with the natural numbers. Curiously enough, when he finally published this approach in 1895, he must have forgotten exactly how he proceeded some nine years earlier, for he ordered the set of positive rational numbers as follows

$$(1/1, 2/1, 1/2, 1/3, 3/1, 4/1, 3/2, 2/3, 1/4, 1/5, 5/1, 6/1, 5/2, 4/3, 3/4, 2/5, 1/6, \ldots)$$

In the mathematical literature, therefore, Cantor is always quoted for his infinite route transposition along alternating diagonals.

In his letter to Goldscheider, Cantor implicitly stresses the fact that the assignment of order is quite arbitrary, provided that it satisfies the basic definition of well-ordering. Within this constraint we can select, according to our fancy, any consistent rule or geometrical pattern. Thus, considering a 2-dimensional array in the form of an infinite table, he ends his illustrations of well-ordering with the following example:

> "*Consider a system of elements* a_{mn} *with two finite but unbounded indices, and determine the rank by the following rule: of two elements* a_{mn} *and* $a_{m'n'}$ *the first has lower or higher rank than the second according as* m *is smaller or larger than* m'; *if, however,* m=m', *the order of ranks is determined by the sizes of* n *and* n'. *This gives the following well-ordered set:*
>
> $(a_{11}, a_{12}, \ldots, a_{1n}, \ldots, a_{21}, a_{22}, \ldots, a_{2n}, \ldots, a_{31}, a_{32}, \ldots, a_{3n}, \ldots, a_{m1}, a_{m2}, \ldots, a_{mn}, \ldots, a_{m+1\,1}, a_{m+1\,2}, \ldots, a_{m+1\,n}, \ldots)$"

Clearly, this is the usual order in which the letters of a page are read. Generalized to tabular arrays of higher, but finite dimensions by Gabriel Kron[25]) in the late 1930s, this is the fundamental ordering later adopted in APL. In view of its importance in array theory as well as in computational practice, we shall denote it the *principal order*. Simultaneously, however, it should be emphasized that principal order is but one out of many ways in which well-ordering may be defined. Transposition ciphers furnish an area of application, based on the study of alternatives to the principal order. Still, as Cantor's diagonal ordering of the rational numbers suggests, cryptography is not the only discipline in which the need for alternative orderings may arise.

From early times, the act of counting a finite collection of things has been identified with the establishment of a one-to-one correspondence with a finite subset of the natural numbers. Galilei's attempt to count the number of square numbers brilliantly extended this method from the finite domain to the infinite. However, the conclusion was so at odds with experience that he felt he had to reject it. Cantor, adopting the same approach, interpreted the conclusion differently. According to him, a set is infinite if it can be put into a one-to-one correspondence with part of itself. The set of natural numbers, therefore, could be used as a measure of the infinity of other sets, adopting the one-to-one correspondence as the basic principle of counting. To describe this measure, he introduced the term *enumerable* for any set which, in this sense of a one-to-one correspondence, contained the same number of elements as that of the positive integers.

Since the integers form a well-ordered set, there will exist at least one well-ordered arrangement of any enumerable set; namely, the arrangement establishing the one-to-one correspondence. This is illustrated by the two diagonal arrange-

ments used by Cantor to prove that the set of positive rational numbers is enumerable. Alternatively, if Cantor had selected the principal order, say, he would not have been able to complete his proof. Thus, since the set of positive integers constitutes the first row in the table of rational numbers (see figure 18A), he would never have been able to finish the establishment of the one-to-one correspondence for this row. It follows that the remaining rows cannot be included in a "count" according to principal order.

Following up on this approach, Cantor began to grade infinity according to size In his correspondence with Dedekind in 1873, he posed the question of whether or not the set of real numbers is enumerable. A few weeks later he was able to demonstrate,[58]) by another type of diagonal approach, that it was non-enumerable. In fact, it turned out to be larger. Later, he discovered that the set of positive integers is the smallest infinite set. However, what is of particular interest to us, is the work he began in 1874 on the equivalence of the points of a line and the points of a n-dimensional space

His aim was to prove that a one-to-one correspondence between these two sets of points was impossible. Three years later he discovered, much to his astonishment, that the two sets were equivalent in size. Taken quite aback at this result of his research, he wrote Dedekind on June 20, 1877: *"I see it, but I do not believe it"*. Hurriedly, he wrote up a paper submitting it to Crelle's Journal on July 12, 1877. To his great annoyance, publication was postponed time and time again in favour of manuscripts submitted later. But if Cantor himself could hardly believe it, how much more difficult would it not have been for the editors to accept it. To their credit, they finally published his contribution in 1878

To give a popular impression of the basic type of approach underlying Cantor's proof, let us set forth a geometrical argument which intuitively demonstrates that the set of points in a square is equivalent to that of the entire plane. [58]) Figure 19 illustrates how we may imagine that the square (shown hatched) is arranged in the XY-plane. Placed upside-down with its top resting on the centerpoint of the square, a pyramid is established such that the centerline through its top is parallel with the Z-axis. Further, the pyramid is turned about this centerline, so that its base is congruent with the square.

Given this arrangement, we first establish a straight line, parallel with the Z-axis, through a point P_i inside the square. This line will cut either a side or an edge of the pyramid in a point Q_i. Extending this approach to all points inside the square, they will be projected onto the surface of the pyramid (including its top, but excluding its base). From the centerpoint W of the base of the pyramid, we now draw a straight line through the point Q_i. This line will cut the XY-plane in the point R_i. Repeating this process, all points on the surface of the pyramid are projected

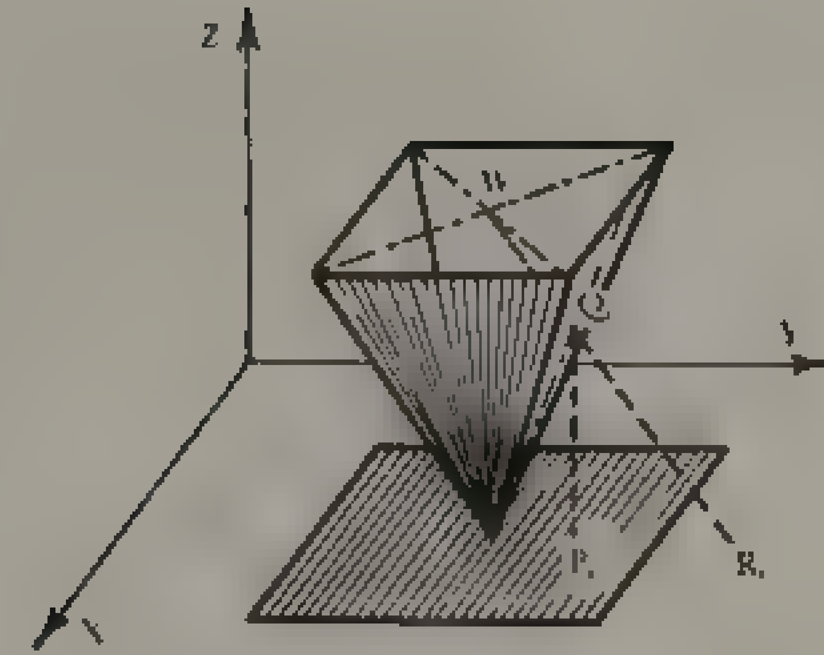


Figure 19. Cantor's proof that a unit square and an infinite plane contain the same number of points.

onto the XY-plane. Thus, by this double projection a one-to-one correspondence has been established between the points P_i inside the square and the points R_i in the XY-plane.

The astounding fact that a line, a plane, and an n-dimensional space contain the same number of points, may be demonstrated along similar lines. Of course, one-to-one correspondences produced in this manner are not continuous; roughly stated, this means that neighbouring points do not necessarily match neighbouring points. Still, the important point is that we can now conceive these infinite entities of different dimensions as reshaping transformations of one and the same geometrical object or manifold. This, then, sustains what we claimed originally; namely, that the array concept may be interpreted as a special type of geometrical space: the finite manifold

Conceived as an abstract object in this geometrical sense, the array shares properties with several other kinds of mathematical objects. Though, we cannot point exactly to one of these well known objects and say that an array is merely this particular object in disguise.

Take a *tensor*, for example. Clearly, an array has that in common with a tensor that we search for geometrical properties which characterize the object independent of the particular coordinate system used to represent and study it. Analytically, we desire to represent these properties by *invariants*. That is, expressions

which retain their form under any change in the coordinate system, and which will consequently have the same value at a given point. To illustrate, if the components of one tensor equal those of another when both are expressed in one coordinate system, they will be equal in all coordinate systems. In particular, if the components vanish (become zero) in one system, they will vanish in all. Equality of tensors is then an invariant with respect to change of reference system.

For arrays, similarly, we can establish equality and other invariants in this sense. But there is a fundamental difference. Arrays must be considered under so general changes of coordinate systems that they include transformations of space from one dimension to another. Transformations of this nature are inconceivable for tensors. Defined by its rank, a tensor is confined to a space of a given dimension only.

Another possibility may be afforded in the branch of mathematics known as *point set topology*. This is a discipline which is concerned with geometrical figures conceived as collection of points with the entire collection often regarded as a space. Again the focus is on the invariance of geometrical properties, but this time under those transformations which deform the figures in any way that does not create new points or fuse existing ones. It was in this discipline that the question of dimension was raised by Cantor's demonstration of a one-to-one correspondence of line and plane; and it was here that Poincaré and others introduced new definitions of dimension applicable to general spaces instead of the tacitly accepted one, namely that it was the number of coordinates needed to fix the points of a space.

The topological transformation of a geometrical figure presupposes that there is a one-to-one correspondence between the points of the original figure and the points of the deformed figure. Equality of the number of points is therefore a combinatorial invariance under these transformations. Evidently, arrays subsume to topological point sets with respect to these properties. There are, however, other topological properties which arrays may, or again may not, satisfy. This is the basic requirement that a topological transformation and its inverse both be continuous. To wit, that nearby points are carried into nearby points. Continuity is the binding property of topological point sets, but for an array to enjoy this property is fortuitous. Thus, the requirement happens to be satisfied for a route transposition by alternating diagonals, but it breaks down under the row and column permutations of a checkerboard alphabet.

Cantor's *well-ordered set* is a third option, repairing the last-mentioned problem. Here, as the name suggests, well-ordering is the relation on the point set. Interpreted as a connectivity property, this relation binds the points together into a space. Confining ourselves to finite sets, we can conceive a transformation from one well-ordered set to another, both with the same number of elements, as the

establishment between the two point sets of a one-to-one correspondence preserving the well-ordering. As implied by its definition, well-ordering presupposes a total or linear ordering of the set. Hence, a convenient aid in the transformation between two well-ordered sets may be to introduce an ordered subset of the natural numbers as an intermediate step. In other words, we use the fact that Cantor's notion of well-ordering originated in the observation that counting, based as it is on the linear ordering of the natural numbers, always proceeds by taking the smallest number in the as yet "unused" set of natural numbers.

Arrays in the form of one-dimensional lists fall into the category of well-ordered point sets. Undoubtedly, some would feel that even this class of arrays is too broad, and that it should be restricted by the requirement that all elements of the array should be distinct. The reason for this is that no two elements of a well-ordered set are the same; each element occurs exactly once.

As we construe it here, however, it is not the values of the array that are of importance. What we wish to emphasize instead, is the positions or "cells", disregarding whatever values they may hold. As we interpret these "cells" or positions, they constitute the point set making up the array. By necessity, all these points are distinct. Their total order is also their principal order, to use the term we introduced for the array-theoretical rule of well-ordering given originally by Cantor.

For a list, of course, the principal order is merely the sequence of natural numbers assigned to the "cells" or positions in counting order. Evidently, this gives rise to a combinatorial invariance between lists of equal number of points. Reintroducing the values in the cells, we may go further and introduce equality between lists as a basic invariant. But that is also about as far as we can go. Arrays of two or higher dimensions and their associated transformations cannot be represented in this manner. Shape or dimension is not an intrinsic property of well-ordered sets.

The conclusion we must draw from this discussion, is that arrays are a novel kind of geometrical manifolds, related to but not identical with the classical types of spaces or geometrical objects studied in mathematics. Whether the point sets of topology, the tensor spaces of differential geometry, or the well-ordered sets of set theory, these manifolds have that in common with arrays that they are point sets in which the points are locally tied together by some binding property known as the connectivity of the manifold.

When in 1854 Gauss assigned Georg Bernhard Riemann the topic of his qualifying lecture for the title of "Privatdozent" at the University of Göttingen, he broke the unwritten rules by taking the last of Riemann's three proposals rather than the first. But Riemann's old professor knew what he did. As Gauss undoubtedly expected, Riemann came to reconsider the whole approach to the study of space in a manner which made him one of the deepest philosophers of geometry.

Geometry	Point set extension	Point identification	Connectivity property
Point set topology	Infinite	Membership function or N-tuple of coordinates	Continuity
Differential geometry	Infinite	N-tuple of coordinates	Infinitesimal Distance
Set theory	Infinite	Membership function	Well-ordering
Array theory	Finite	N-tuple of coordinates	Well-ordering

Figure 20. Geometrical manifolds based on the Principle of Local Simplicity

Endeavouring to show that Euclid's particular axioms were empirical rather than, as had been believed, self-evident truths, he rejected the considerations of space as a whole, as it was found not only in Euclidean geometry but also in the non-Euclidean geometries of Gauss, Bolyai, and Lobatchevsky. Instead, he claimed that we know space only locally. This led him to advocate Grassmann's concept of a manifold, as mentioned earlier, and to the introduction of infinitesimal distance as the simplest possible property defining the connectivity of space. Einstein's dictum: "*Physics is simple only when viewed locally*", is therefore a geometrical principle originating with Riemann. Other mathematicians substituted infinitesimal distance by various binding properties, such as continuity in point set topology, and well-ordering in set theory. In the course of events, it was gradually realized that, basically, they were all satisfying the same *principle of local simplicity*.

Figure 20 attempts to describe the kinds of manifolds characteristic of the three more important geometries based on this principle. Columnwise, apart from the extension of the point sets and their connectivity properties, it is also shown how the points are identified: either by giving their coordinates, or by specifying some definite propositional function for deciding their membership by yes or no. The fact that the extension of a point set is given as infinite, does not exclude finite point sets. The addition of a row for arrays to this description brings explicitly to the fore, that we have here a new combination of the basic properties defining a geometrical space. Perhaps more clearly than we have been able to do it before, this demonstrates that array theory is a novel geometry, arisen from the experience with data.

When Euclid compiled the 13 parts of his immortal *Elements* about 300 B.C., he made every effort not to rely on unsupported intuition or on mere physical experience. To him like to most other Greek philosophers of antiquity, the study of geometry was truly a highway to the world of ideas. One did not profane this science by using it to earn money. Nor did one demean it by applying it to technical problems. Thus, Plutarch reports that Plato accused mathematicians such as Eudoxus and Archytas of "*lowering the dignity of geometry by letting it sink from the immaterial and intellectual to the material*", because they dared use geometry to solve mechanical problems. Still, as recounted above, Riemann did not hesitate to declare Euclid's axioms empirical; and for good reasons too. Euclid's work would not have been possible at all without the collective contributions of unknown men who, in the preceding centuries, abstracted the basic ideas and notions from observations of reality.

Considering the astounding feat that the *Elements* was a textbook in common use for over 2000 years, it is not surprising that its general view on what constitutes mathematical method should dominate our thinking. But what is surprising, is that it does so to the degree that so many of the great mathematical inventors, forming the link from Euclid until today, should feel obliged in their writings to erase any trace of how they arrived at their results.

In his *Passages*, Babbage declared that, "*The great object of all my inquiries has ever been to endeavour to ascertain those laws of thought by which man makes discoveries*". As we have seen in the discussion of his *The Philosophy of Analysis*, this was also the avowed goal of his mathematical inquiries. Whereever his many-varied interests would take him, from games and ciphers to his beloved Engines and other mechanical contraptions, Babbage constantly found inspiration to create novel ideas and abstract generalizations. A letter from Archimedes to Eratosthenes on the process of geometrical discovery might therefore have interested him. In particular, since Archimedes' demonstrations of geometrical theorems, for instance in his writings on *Sphere and Cylinder*, would seem impossible for anybody else to invent, even if his proofs are of an exemplary clarity, completeness, and elegance.

The letter was discovered in 1906 in Constantinople by Johan Ludvig Heiberg, a classical philologist who earned his living as a gymnasium teacher at Østre Borgerdydskole in Copenhagen. [60]) He had a scientific reputation in the international literature because, during the years 1883-1888, he published the genuine text of Euclid having restored it after many years of source studies; most Danes would nevertheless associate him with some classical and delightful vaudevilles, still on the repertoire of the Royal Theatre in Copenhagen. They would erroneously believe

him to be an antecedent namesake of his, the famous author and playwright, whose paternal uncle happened to be the great-grandfather of the philologist. Anyhow, when our Heiberg stumbled on this letter, often termed the Constantinople manuscript, he immediately recognized its importance and rescued it for posterity. In it, Archimedes explains how he often attained insight into geometrical relationships by means of mechanical considerations: [59])

> "*Certain theorems first became clear to me by means of a mechanical method. Then, however, they had to be proved geometrically since the method provided no real proof. It is obviously easier to find a proof when we have already learned something about the question by means of the method, than it is to find one without such advance knowledge. That is why, for example, we must give Democritus, who was the first to state the theorems that the cone is a third of the cylinder and the pyramid of the prism, as much credit as we give to Eudoxus, who was the first to prove them.*"

Although the array concept has roots far back in mathematical history, the first to single them out and describe them as geometrical objects was undoubtedly Gabriel Kron in his pioneering work of the 1930s. [51]) Recognizing that they were not tensors though of a related nature, he introduced his so-called *Generalization Postulates* to capture what we would now call array invariants. Somewhat of a scientific autodidact, Kron presented his ideas more like a political campaigner than as a scientist, and he soon became the centre of a fierce battle raging almost to his death in 1968. It was readily demonstrated that his "postulates" were not at all postulates in the Euclidean sense. But nobody, apart from a few individuals, recognized in their formulation valuable heuristic guidelines for identification of array-theoretical invariants. One mathematician, J. Slepian, even mocked his work by calling his geometrical objects "*fruit salad*", and it took all the authority of Banesh Hoffmann, a tensor specialist co-authoring some of Einstein's papers, to defend and explain Kron's approach

However, it was Kenneth E. Iverson's remarkable book, *A Programming Language*, published 1962, and the subsequent implementation on the computer of Iverson's operational notation for mathematics, now abbreviated to the acronym *APL*, which provided the empirical basis for the general acceptance of a geometrical theory of data. By the title of this book Iverson intended to convey its content as the introduction of an "*effective notation*" in applied mathematics. Inspired by a variety of mathematical disciplines, he focused on arrays of data, then termed "*structured operands*", saying: [61])

> "*Any operation defined on a single operand can be generalized to apply to each member of an array of related operands. Similarly, any binary operation (defined on two operands) can be generalized to apply to pairs of corresponding elements of two arrays. Since algorithms commonly incorporate processes which are repeated on each member of an array of operands, such generalization permits effective subordination of detail in their description*".

Iverson's approach was purely heuristic. Beneath it we find no unifying theory. Of course, there are many theoretical subjects, in particular matrix algebra, taken from various branches of mathematics. But the beauty of it all is the way in which this multitude of topics comes together in a harmonious whole subsuming to a simple set of elegant, yet pragmatic rules rigidly adhered to. Playing Euclid for a minute, we may ask ourselves why it is, that Iverson and the other originators of APL as a computer language found these empirical rules so important or self-evident that, collectively, they felt obliged to abide by them. Could it be that, intuitively, they recognized beneath these rules certain basic truths, amenable to be interpreted by us as array invariants.

It is a common observation that storing an n-dimensional array of data in a computer is tantamount to its transformation into a list or one-dimensional array. Thus, remarking in his book that "*any structured operand can first be reduced to an equivalent vector*", Iverson introduced, as part of his notation, a special terminology for this equivalent vector of an operand "*x*", calling it the "*representation of a quantity x*" and denoting it "*ρ(x)*", so as to be able to describe mathematically the allocation of the operand on the physical storage elements of the computer. Seemingly, it is an insignificant step to use a mathematical mapping to denote what until then was considered merely an engineering expedient to overcome the physical constraints of the computer. It is therefore thought-provoking that the team around Iverson at IBM, developing APL as a computer language, should concentrate on this mathematical idea and, even taking over the notation, should adopt it in a generalized form as a fundamental design principle.

The so-called *dimensional identity* in figure 21 captures this array invariance in a single APL statement. [62]) It says in plain words that any array: "*A*" (specified on the left hand side) is equal to its *ravel:* ",*A*" or the list of its elements in total order (on the right hand side), reshaped back into an array as determined by its *shape* or

```
IN APL THE BASIC INVARIANTS OF ARRAY  A  ARE

  DIMENSIONAL IDENTITY          A = (ρA)ρ,A
  COMBINATORIAL IDENTITY  (×/ρA) = ρ,A

WITH THE STRUCTURAL OPERATIONS
  RAVE    ,A   SHAPE. ρA   &   RESHAPE  DρA
AND THE SCALAR PRODUCT OF THE DIMENSIONS  D
               REDUCTION   ×/D
```

Figure 21. Invariants in APL.

vector of dimensions "ρA". Experienced APL users may note here that, although the *reshape* operation: "$D\rho A$" will interpret its right argument as the ravel of that argument in any implementation, this is merely a convenient shorthand notation for the expression given in the figure. The remarkable fact, which may be verified by experiments on the APL terminal, is that this identity holds *without exception* for all arrays, whether scalars (i.e. single numbers or characters), tabular and nested arrays, or even something as exotic as empty arrays. Without this identity, APL would have been just another programming language. With it, perhaps the most decisive step was taken towards the formulation of a geometry of data-structures, and the establishment of an associated fundamental algebra of data.

The combinatorial identity given in the figure for tabular arrays, may be considered a corollary to the first mentioned identity. All it states, is that the total number of elements is preserved under the transformation. Thus, on the right hand side this number is determined by the length or dimension of the totally ordered list of elements, while on the left hand side it is found multiplying together the lengths or dimensions of the axes, in exactly the same way that we determine the area of a rectangle or the volume of a box.

In his *Passages*, Babbage recounts a few of the more remarkable questions he had been asked with respect to his Difference Engine:

> "*One gentleman adressed me thus: 'Pray, Mr. Babbage, can you explain to me in two words what is the principle of this machine?' Had the querist possessed a moderate acquaintance with mathematics I might in four words have conveyed to him the required information by answering, 'The method of differences'. The question might indeed have been answered with six characters thus –*
>
> $$\Delta^7 u_x = 0$$
>
> *but such information would have been unintelligible to such inquirers*

The method of differences, used as design principle for Babbage's first computer, is an approximating technique for determining mathematical, astronomical, or other tables by a repeated process of addition. [63] The abstract idea underlying each step of this process, has an intuitively simple illustration for a chronological table of events. Namely, that the difference between the dates of two adjacent events carries physical meaning as a timespan or length measured in number of days, months, or years. Had Babbage's Difference Engine been completed, it would have been able to accomodate six such orders of differences, the last one being merely the same constant value over all the adjacent pairs of fifth order differences. His mathematical statement, that the seventh order difference would vanish (become zero), was therefore an apt description of his computer. It represented the maximum technical capability by an invariant.

By analogy, we may say that the dimensional identity is a succinct characterization of APL. Yet, conceived as an algebraic invariant, it is of far deeper significance. Like a vector or tensor equation, its form is preserved independent of any choice of coordinate system or whether the array is tabular or nested. Further, like in such equations its value in any given point is preserved in the sense that only the shape of the array is changed. That is, the number of points or cells and their values remain invariant.

Perhaps most important is the fact that, although developed and integrated into APL, the dimensional identity is completely independent of this language. Apart from our arbitrary choice of adopting the APL notation, the identity is truly an array-theoretical invariant based on the inverse pair of transformations, the ravel: "$,A$" and the reshape: "$D\rho A$". All that is specified about these two transformations, is that they establish a one-to-one correspondence between points and preserve the connectivity property of well-ordering. That APL happened to use the rule of principal order for the latter binding property, is from our point of view an entirely arbitrary choice. In set theory, for example, exactly the opposite rule of principal order happens to be used to sequence Cartesian products of totally ordered sets. Since adherence to the rule of principal order would give a *lexicographical ordering* in this application, the resulting set-theoretical ordering is known as an *anti-lexicographical ordering*. [64] However, the actual choice of rule need not be related at all to the notion of principal order. Whatever we find convenient or appropriate for one reason or another will do, in so far as it satisfies the basic requirement of well-ordering.

The very fact that the dimensional identity is thus open to interpretation, brings us back to the question of cryptographical data transformations. Transposition ciphers by "*equal letters*", as Bishop Wilkins termed it, is clearly an area of a long and venerable tradition for exercising the freedom of choice in selecting a suitable rule alternative to principal order. The requirement of equal letters is but a specification of the one-to-one correspondence between points. The positions of the letters in the plaintext conceived as a list, constitute their total order as it is related to a sequence of natural numbers. Hence, the letters of the plaintext are well-ordered. Denoting the rule specified by a cipher its *transposition order*, to distinguish it from the concept of principal order, it is readily seen that the reshape operation may be interpreted as *enciphering*, and the ravel operation as *deciphering*. That is, the array "A" represents the cryptogram or the enciphered text, and its ravel, "$,A$" the plaintext. It is noteworthy that, as a special case, the array "A" may be even a list, reordered in relation to the plaintext.

It is well known from other branches of mathematics that one and the same relationship or equation may be given different kinds of interpretations depending

on the problem at hand. The power of a mathematical representation is that it is neutral with respect to its application. It should not surprise us, therefore, that the dimensional identity, being an abstract geometrical invariant, should have a cryptographical interpretation different from that installed in our minds by the use of APL.

An important advantage of this array-theoretical representation of transposition ciphers, is the fact that it explains why the study of substitution ciphers may be confined to plaintexts in the form of lists. Evidently, this follows from the dimensional identity which tells us that the transformation of shape preserves all component values of an array. Dealing with transformations of component values, we can therefore neglect the problem of shape transformations, picking for our discussion the shape that we find most convenient. Of course, this shape is the list.

2.9 The Erlanger Program

In the same period 1870-72, in which Cantor began to devote his professional life to the measuring of the "infinite", another young German mathematician declared it his goal to measure the intuitive notion of "invariance". Like Cantor, he was inspired by Riemann's qualifying contributions in 1854 for the title of "Privatdozent"; but where Cantor took his starting point in the paper submitted by Riemann, extending the representation of functions by arbitrary trigonometric series to cases of an infinity of exceptional values, our young man was motivated by Riemann's public lecture on the hypotheses underlying geometry.

However, it was not only in their selection of topic area but also in their fundamental attitude that the two men differed. When Cantor claimed in 1883 that "*The essence of mathematics lies in its freedom*", thus divorcing this discipline from reality, our other mathematician, the equally famous Felix Klein, pointed out that "*whoever has the privilege of freedom should also bear the responsibility*", thereby discarding all such mathematics which did not serve in the investigation of nature.

It appears to be a general observation in the history of science, that invention of a novel kind of measurement is a fountainhead of important conquests. This statement also holds true here. Klein's contribution wrought a revolution, first in geometry, and later in physics and chemistry, no less impressive than that which Cantor brought about in pure mathematics.

Although Einstein did not realize it about 1915 when he developed his general theory of relativity, Klein's measure of invariance provided a royal road to his novel formulation of the conservation laws of energy and momentum. In fact, this was the celebrated theorem of Emmy Noether which, published in 1918, is now an

essential tool in theoretical physics. [65]) Over the years since this initial success, Klein's measure of invariance has come to dominate the modern theoretical development of physics and chemistry. The question therefore arises, whether we can expect to see a similar impact upon other, more application-oriented disciplines.

To predict by reasoning, is the ultimate aim of any scientific model or theory. Yet, logical conclusions about reality can only be deduced if the model or the theory provides a consistent description of the observed regularities or repetitions in the functioning of natural or man-made systems. The importance of Klein's measure of invariance, is that it provides an abstract mathematical tool for capturing such observed patterns. Not only does this permit us to identify or recognize such patterns and draw upon experience by analogy to other disciplines, but selecting a geometrical or other suitable image or representation, we can gain insight aiding us in the design of a particular system.

In the traditional engineering disciplines, we can rely upon the natural laws of the underlying physics in our system design. Similarly in economics, we attempt to base the theory on the laws of social or psychological behaviour. Still, surprising as it may seem, there are many highly-developed areas for which we have failed so far to establish "laws" in this fundamental sense. It is in areas of the latter kind, such as automatic control [54]), or factory management systems, [66]) that we now find initial attempts at coping with complexity invoking Klein's tool. Cryptography is another area where, as we shall see later, Babbage's early attempt at establishing a law found its final expression as an invariant in the sense of Klein in the independent contribution of de Viaris in 1888. Yet, most important, because it will influence the daily work of the largest number of people by far, is the relationship between Klein's measure and the geometrical notion of a data array. [51])

In 1872, when Klein was appointed to the University of Erlangen, it was still expected that a new professor had something to profess, namely a research program. This Klein lived up to in his inaugural address: "*Vergleichende Betrachtungen über neuere geometrische Forschungen*" (A Comparative Review of Recent Researches in Geometry). Perhaps the most famous research declaration of its kind, this address is known today simply as the *Erlanger Program*, using the German colloquial form: "Erlanger" rather than the grammatically correct, but perhaps more pedantic term: "Erlangener". [67])

Measurement is basically an act of comparison with some scale. Hence, to devise a gauge we have to decide upon two things: the rule governing the act or process of comparison, and the choice of the measurement scale itself. Before these two things can be decided upon, we must of course agree as to the principle underlying the measurement. To get the bright idea here is important, because it determines how simple and convenient we may proceed. Take, for example, Cantor's measure-

ment of the "infinite" His bright idea was to adopt counting as the principle of measurement. Therefore, it followed almost naturally that the act of comparison had to be by a process of one-to-one correspondence with a scale of the natural numbers.

For Klein, attempting to measure invariance, the inspiration arose out of his interest in geometry. Pondering the question of what constitutes an objective description of invariance, he arrived at a surprising, yet obvious answer. What we commonly observe and are able to compare, when we claim something to be invariant, is that after certain things have been done to it, it looks the same as it did before. To be sure, since we cannot distinguish between what we have now and what we had before, it is for all scientific purposes the same – it is invariant. Klein concluded, therefore, that the underlying principle of measurement had to be based on some kind of enumeration or classification of all the things, let us call them: *transformations*, which possibly could be invoked without destroying the invariance. Further, to identify some distinct property which might serve as a scale of measurement for metric as well as for non-metric invariances, he consulted geometry for analogies. Considering various transformations that left figures invariant, such as turning a square around through 90 degrees, or exchanging its right and left sides, he soon realized that what characterizes an invariance is some characteristic symmetry.

Symmetry seems always to have fascinated the human mind. [67]) By way of Latin, the word comes from the Greek term: *summetria*, meaning "of like measure", which was interpreted by the ancients as an aesthetic principle of balanced proportions, or harmony of arrangement. Thus, Plotinus in his famous book *Aesthetic*, in the First Ennead, Vol. 6, Chapter 1, said: *"Now almost by all persons it is maintained, that it is the* symmetry *of the different parts with respect to each other, and the beautiful colour, which produce* beauty *for visual observation; and for those as well as for the common intellect* beauty *is identical with* symmetry *and being shaped after fixed proportions"*

Clearly, as an aesthetic principle in decorative art and architecture, the word symmetry was used to convey the visual impression of some geometrical regularity, or some process of repetition which externally manifested itself in various forms or figures. Since geometry could be used for the abstract and idealized study of symmetry, this explains the classical belief in this discipline as a tool for the exploration of the world of ideas. Representing numbers by geometrical arrangements of pebbles as reflected nowadays in terms like "even", "odd", and "square numbers", or ordering the pitch of string instruments according to the ratios between geometrical lengths of the strings, the ancient Greeks extended the abstract notion of symmetry beyond the geometrically visible. From this first step and up to Klein's Erlanger Program we find a steady evolution, making symmetry one of the most

important formal notions in mathematics and the associated sciences. However, before we return to Klein's use of symmetry as a measure of invariance, I would like briefly to touch upon the question of asymmetry.

Some years ago, a modern British painter, Francis Bacon, I believe, declared in an interview that he would never paint more than one person on his canvass because otherwise it would create too much symmetry. This statement is significant because it reflects a very fundamental human attitude. Asymmetry, as we perceive it, is not merely the absence of symmetry. As the mathematician Weyl has expressed it in his discussion of the mosaic of an Etruscan tomb: [68]) *"Even in asymmetric designs one feels symmetry as the norm from which one deviates under the influence of forces of non-formal character"*.

What is thought-provoking here, is that it is the deviation from symmetry which also in physics and chemistry provides new valuable knowledge. For instance, it was important in the past to discover that instead of the assumed spherical symmetry of the earth, there was a flattening of the poles, because it confirmed its rotation around an axis through the poles. Recounting how he discovered piezo-electricity merely by theoretical reasoning about symmetry, Pierre Curie, the husband of Marie Curie and co-discoverer of radium, coined his famous dictum: *"It is dissymmetry that produces the phenomenon"*. When James Clerk Maxwell formulated his celebrated laws of electromagnetism, his only reason for introducing an additional term, calling it the displacement current, was that it made his equations algebraically symmetrical; and yet, it lasted almost twenty years before another physicist, Heinrich Hertz, was able to confirm the new phenomenon by experiment. Similarly, in his work Einstein would argue: *"from reasons of symmetry"*. What this illustrates, is that whenever these men encountered dissymmetry, they would modify their description of reality in such a way that, by taking into account the hitherto neglected fact, symmetry would again be restored. Such is the belief in symmetry as a scientific tool of exploration.

The essence of the Erlanger Program is that it formalized this belief. Like all other statements in science since Galilei, it explains *how*, not why. During his student days in Paris, Klein had formed a fast friendship with Sophus Lie, the Norwegian mathematician, with whom he had been working over a number of years prior to the enunciation of the Erlanger Program. Lie's great interest was group theory, and his contribution to this branch of mathematics was such that he gave name to the so-called *Lie Groups*. Undoubtedly, it was the profound knowledge of group theory acquired through this friendship which inspired Klein to introduce this abstract tool as his gauge of invariance.

The idea of a group goes back to Évariste Galois, who died in a duel in 1832 at the age of twenty-one. However, it was Arthur Cayley who in 1854 generalized the

concept and introduced the notion of an *abstract* group. [69]) Although somewhat archaic in its presentation, Cayley's delightful paper might fit well into the chapter on group theory in any mathematics textbook of today's highschool or gymnasium, thereby convincing anyone that the expression "modern math" must be taken with a grain of salt.

The essence of the concept, as explained by Cayley, is really very simple. Imagining a table for multiplication (or addition) of the natural numbers by themselves, all we are required to do is to extend this idea of a *multiplication table* to "products" of some list of distinct symbols, say letters, by themselves. To fix ideas, let us say that this list of symbols, the so-called *carrier*, represents the entire set of spatial transformations which would leave a given geometrical object invariant. With this interpretation, let us further define the "product" "*BA*" of two arbitrary transformations "*A*" and "*B*" to mean, slightly changing Cayley's terminology, the compound transformation, the performance of which is equivalent to the performance, first of the transformation "*A*", and then of the transformation "*B*". Thus, reading from right to left as in APL, Cayley may be said to interpret the "product" as the operation: *"followed by"*

The change in view of the symmetry concept from the ancient Greeks to the nineteenth century mathematicians, may appear a mere twist in perception. Originally, symmetry described the observation of a spatial or temporal repetition of similar elements. The novel idea was to interpret the concept as an *operation*, a movement whose point of ending is indistinguisable from its point of beginning Far from being trivial, this change made possible a consequential algebra of symmetry. An algebra which has its genesis in the fact that we can "*multiply*" two such motions by performing them in succession

Cayley's multiplication table provides a concise description of this kind of multiplication of motions. If the set of distinct motions, the carrier, is infinite, the table too will be infinite. Otherwise, the table is finite. The latter condition will be assumed to be satisfied in the following. With the set of row indices and the set of column indices, each specified by the carrier or set of possible motions, an entry in the table will define the product of that particular pair of motions which is identified by the corresponding pair of row and column indices. That is, the entry is but the single motion which accomplishes exactly the same transformation as the successive performance of the two motions creating the product. Thus interpreted, there is no difference in principle between Cayley's table and the conventional table for addition of the natural numbers. Indeed, it makes as much sense to say that a rotation of a square first by 90 degrees and then by 180 degrees is tantamount to a resulting rotation by 270 degrees, as it does to say that counting first to 90, and from there on 180 more, is the same as counting directly to 270. However,

there is also a difference which, albeit quite subtle, is of fundamental importance.

It is commonplace that the operands of an addition table are merely abstract objects, namely the numeral numbers. In fact, when we think about operations in any physical or geometrical sense, they always apply to operands which we can describe as "things" or entities, usually interpreted as objects or events. Yet, if we take a careful look at the operands in Cayley's table, we recognize that basically they are operations; but what operands they again are performed on, is not part of the description in the table. Perhaps this is what inspired the mathematician Charles Lutwidge Dodgson, on that famous picnic near Godstow on July 4th, 1862, when he told Alice Liddell and her two sisters about the grin of the Cheshire Cat in the now famous story *Alice in Wonderland*, published later under his nom de plume, Lewis Carroll: [70])

> *"I said pig", replied Alice; "and I wish you wouldn't keep appearing and vanishing so suddenly. You make one quite giddy".*
>
> *"All right", said the Cat; and this time it vanished quite slowly, beginning with the end of the tail, and ending with the grin, which remained some time after the rest of it had gone.*
>
> *"Well! I've often seen a cat without a grin", thought Alice; "but a grin without a cat! It's the most curious thing I ever saw in all my life!"*

The change in our conception of symmetry is no less curious. We have arrived at the notion of a multiplication table each operand of which is really a symmetry interpreted as an operation; but from the actual information in the table, we cannot tell the symmetry of what. It is this generalization which creates a measure of symmetry independent of the particular application. Of course, we have the same independence of application in the table for addition of the natural numbers. Neither here, do we know the number of what. Yet, the remarkable difference is that to achieve this advantage in the case of symmetry, we had to generalize the concept of a multiplication table from "products" of operands to "products" of operations. This was a tremendous step in abstract thinking. A leap, testifying to the ingenuity, the imagination, and the intellectual courage of the great contributors at the time.

When mathematicians talk about *"structure"*, the word has a precise meaning adopted throughout all the sciences. By structure they mean the relations between the elements and the operations of a set. Whatever properties we can ascribe to Cayley's multiplication table, they form the structure of executing in succession the symmetries that we have collected in the set called the carrier. Since relations and multiplication tables can be established for numbers as well as for geometrical entities, it is easy to visualize that multiplication tables (and hence groups) can be

used to measure the symmetry not only of geometric figures but also of algebraic systems. Comparing tables, we simply identify a given structure by its distinct pattern or relations. Our situation resembles that of Alice,

> *"when she noticed a curious appearance in the air: it puzzled her very much at first, but, after watching it a minute or two, she made it out to be a grin, and she said to herself, It's the Cheshire Cat: now I shall have somebody to talk to".*

Depending upon the application, the same abstract structure of a multiplication table (or group) may be given different representations. In some respects these representations may be considered analogous to the use of coordinates in the treatment of geometrical problems. The earlier literature on the subject, including the classical works of Cauchy, Galois, Jordan, and Julius Petersen dealt exclusively with representations in terms of permutations. That is, a rearrangement of a set of distinct objects among themselves.

Mathematically, a *permutation* is defined as a one-to-one mapping of a finite set of elements into itself. Thus, for example, we may label the four symmetrical parts of a geometrical figure by the sequence of the first four natural numbers, and then describe a symmetry operation empirically by whatever facts we observe, say, that part 1 is replaced by part 3, part 2 by part 4, etc., writing the permutation:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

to indicate that each number in the upper row is to be replaced by the number immediately below it in the lower row.

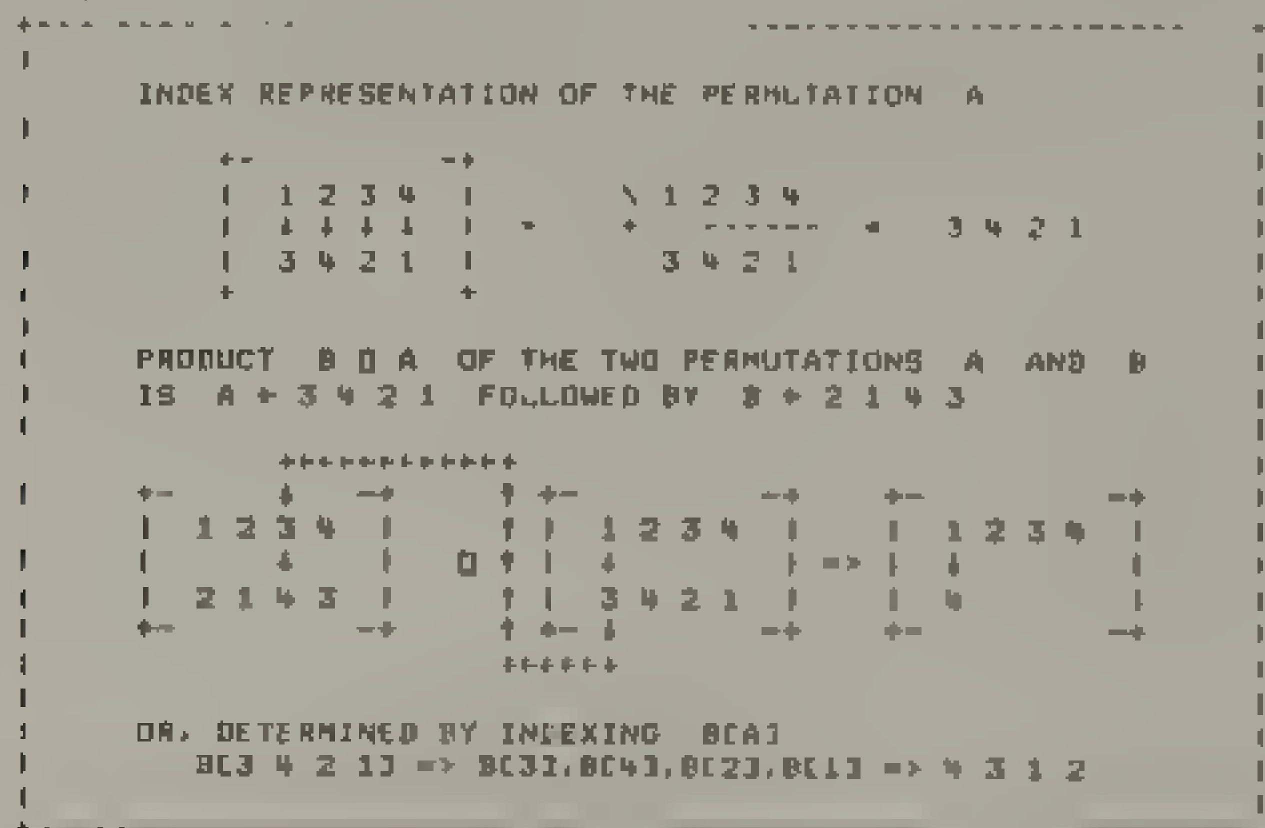


Figure 22. Computing permutations by indexing.

Figure 22 demonstrates how this conventional mathematical notation may be made operational in APL, if we simply write the permutations as vectors and use the indexing of such vectors to represent products of permutations. In particular, considering the figure, we find for the product "*BA*" by a trace of the arrows, beginning at permutation "*A*", that 1 is mapped to 3 and, ending at permutation "*B*", that 3 is mapped to 4, so under the product "*BA*" 1 is mapped to 4 as shown to the extreme right. Incidentally, this order of execution from right to left does not only fit APL, but it also agrees with our notion of composition of a pair of mathematical functions "*g*" and "*f*" because:

$$(gf)[x] = g[f[x]]$$

Though, I must warn the reader that some authors adhere to the opposite order performing such products of permutations.

All the early expositions of group theory were based on representations in terms of permutations, which had been derived from labelling the symmetric parts by a sequence of positive integers, forming a set of non-metrical coordinates. Since the permutations described symmetries by substitution of one part for another, the older literature used to call this branch of mathematics *substitution theory* or *substitution analysis*. [71]) Similarly, the *permutation groups* were termed *substitution groups*. The aim in all the first applications was to investigate the solution of algebraic equations. Here, therefore, the roots of such equations appeared as the symmetric parts, which were labelled and submitted to permutations. In his book from 1877, Julius Petersen gives a fascinating introduction to this topic which, though of far more than just historical interest, is rarely dealt with in our modern mathematics textbooks. [72])

In the second part of his paper from 1854, Cayley demonstrated a famous theorem now named after him. [69]) It says that any finite group whatsoever can be represented by a suitable group of permutations. This made the group of all permutations of *n* elements the most general and all-embracing group, because it contained all other finite groups as subgroups. In view of its origin in the description of symmetry operations, it was termed the *symmetric group*.

In this discussion, I have interchangeably used the words group and multiplication table, reflecting the attitude of the first mathematicians working in this area. They believed that all that sensibly could be a multiplication table, would also form a group. Hence, they derived the laws composing the structure of a group by inspection of the table. For example, by analogy to the addition or multiplication tables of natural numbers, they concluded that every element ought to have an inverse element, so that by multiplication of an element by its inverse, the identity or neutral element would result. Similarly, the multiplication of an element by the identity element will leave the element unaltered.

Figure 23 (see page 134) gives a simple illustration of this classical approach, yet clothed in APL indexing operations. We shall rely on this example in much of our future discussion and, however strange it may seem now, it will be central to our explanation of Babbage's attempt at throwing cryptography into a mathematical framework. Hence, although the figure is self-explanatory, I would like to add a few remarks

First, to admit the necessary identity or neutral element, we have to include the strategy of doing nothing This is in agreement with the fundamental dictum of economic decision theory that not to do anything, is also to make a decision. Secondly, if we consider a single arrow in the arrow diagrams defining the strategies, we will assign meaning to it by a causal rule of *immediate succession*. That is, the position at the head of the arrow is the immediate successor to the position at the tail of the arrow In other words, an arrow relates the two positions of a tire, namely after (the arrow head) and before (the arrow tail) the execution of the strategy in question Clearly, it is in this way that we can identify a symmetry as an operation and represent it by a permutation. Thirdly, we conceive the multiplication table as produced in principle as an APL outer product of the carrier by itself. Thus, since the neutral element is the first in the carrier, the first row and the first column of the table will reproduce the carrier. We also note that the table, therefore, satisfies the law of *closure*.

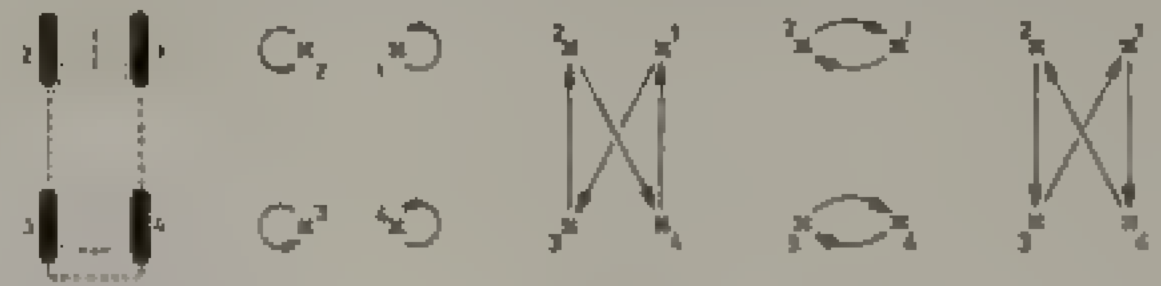
The APL indexing representations of the permutations and their products, have been explained already in figure 22. What is new, is that the inverse of a permutation can be determined directly, invoking the APL grade-up function. This function grades the elements of a vector in ascending order, so that in the result the first element is the index of the smallest element in the vector, the second element is the index of the smallest element but one, etc. The test whether or not the commutative law is satisfied, proceeds by a Boolean comparison which has to be true for all pairs of corresponding elements. Camille Jordan, in his famous book: *Traité des substitutions et des équations algébraiques*, published 1870 , introduced the designation *Abelian* for a commutative group in honour of the Norwegian mathematician Niels Henrik Abel. Of course, to verify that the multiplication table does indeed form a group, every test in figure 23 has to be repeated for all possible products. If this is done, as anyone may convince himself, these tests will come out in the affirmative

Arrow diagrams of the kind used here to define the strategies, are known in the mathematical literature as *directed graphs*, or *digraphs* for short. The term "graph" used in this sense was introduced by James Joseph Sylvester in a note he published in February 1878. [48]) Like his friend Cayley who already in 1857 wrote about "*Analytical Forms Called Trees*", Sylvester was much occupied with the so-called *graphic notation*, which over the decade 1854 to 1864 had been introduced by chemists such as the German F. A. Kekulé and the Scot A. Crum Brown to describe chemical compounds diagrammatically. There can be little doubt that Sylvester derived the word "graph" from the chemical "graphic notation". Geometrically, a digraph is composed of two types of objects: points and arrows, technically known as *vertices* and *directed edges*, respectively. If it is desirable to emphasize that the arrows represent the relationship of immediate succession, the term *successor digraph* may be applied. Correspondingly, one may talk about *predecessor digraphs*.

Digraphs are one of the most versatile and useful tools in modern data handling, so it will be worthwhile to digress a bit in order to demonstrate how elegantly they may be represented algebraically in APL in terms of logical or Boolean matrices. This is demonstrated in figure 24, where the digraph of each strategy in the automobile example is represented by a Boolean *successor matrix*. That is, a matrix in which the entries are assigned the truth values: "1" for true, or "0" for false, depending upon whether or not there exists an arrow between the two points of any pair of points. To be sure, if "*I*" is a row index and "*J*" a column index of such a Boolean matrix "*M*", then an entry: "$1 = M[I;J]$" signifies that vertex "*I*" is the *immediate successor* of vertex "*J*", or that there is an arrow from vertex "*J*" to vertex "*I*" in the corresponding digraph. A special case of this rule, illustrated by the neutral strategy, is an entry: "$1 = M[I;I]$" which represents a particular kind of arrow, called a *loop*, with the same vertex "*I*" as both initial and final vertex. Apart from the situation, in practice unusual, that there is more than one arrow from some vertex to another, this approach establishes, a on-to-one correspondence between any digraph and its associated Boolean matrix representation. In particular, if the digraph has the very special property that each vertex has only one arrow going out and only one arrow coming in, it will be represented algebraically by a special Boolean matrix known as a *permutation matrix*. This is a matrix which has one and only one entry "1" in each row and each column and "0" elsewhere. It is readily appreciated that the four strategies give rise to such digraph representations.

The advantage of this representation, is that there exists a consequential matrix algebra of symbolic logic, a *Boolean matrix calculus of relations*, which we can now apply. [49]) The matrix product of this algebra, known as the *relative product*, is defined by analogy to the conventional Cartesian matrix product. This is shown in figure 25. The remarkable power of APL's inner product explicitly to denote the two basic operations involved: a summation and a scalar product, brings out this similarity in a very concise way. Thus, we immediately perceive that Boolean algebra substitutes the conventional multiplication by the logical connective "*and*" *(conjunction)* and the conventional summation by the logical connective "*or*" *(disjunction)* The name "relative product" originates in the fact that the Boolean matrices in

```
A CLASSICAL PROBLEM IS THE INTERCHANGING OF THE FOUR
TIRES OF AN AUTOMOBILE TO ACHIEVE AN EQUAL DEGREE OF
WEAR.  A SET OF POSSIBLE STRATEGIES, INCLUDING THE
USUAL OPTION OF DOING NOTHING, MAY BE THE FOLLOWING
```




```
DEFINING THE PRODUCT OF TWO STRATEGIES    XDY   AS
STRATEGY "Y" FOLLOWED BY STRATEGY  X , WE FIND BY
VISUAL INSPECTION THAT THE POSSIBLE COMBINATIONS OF
THE FOUR STRATEGIES FORM THE MULTIPLICATION TABLE

      +---+     +---------+            \ E A B C
      | E | ∘.D | E A B C |           --+-------
      | A |     +---------+           E | E A B C
      | B |                     =>    A | A B C E
      | C |                           B | B C E A
      +---+                           C | C E A B

IF EACH STRATEGY IS REPRESENTED BY THE PERMUTATION
IT PRODUCES OF THE POSITIONS OF THE TIRES
E←1 2 3 4     A←3 4 2 1     B←2 1 4 3     C←4 3 1 2

THEN THE  PRODUCT  OF TWO PERMUTATIONS IS FOUND AS
THEIR SUCCESSIVE PERFORMANCE IN PARANTHESIZED ORDER
      B[A]                A[B]                C[B]
4 3 1 2             4 3 1 2             3 4 2 1

THE PRODUCT IS ASSOCIATIVE
      C[B[A]]             (C[B])[A]
2 1 4 3             2 1 4 3

AND COMMUTATIVE
      ∧/B[A]=A[B]
1

THE NEUTRAL STRATEGY  E  IS THE IDENTITY ELEMENT
      E                   A[E]                E[A]
1 2 3 4             3 4 2 1             3 4 2 1

EACH PERMUTATION  X  HAS AN INVERSE ELEMENT   ⍋X :
      ⍋A                  A[⍋A]               (⍋A)[A]
4 3 1 2             1 2 3 4             1 2 3 4
```


Figure 23 The automobile example

```
EVERY FINITE GROUP CAN BE REPRESENTED  ACCORDING TO
TO CAYLEY S THEOREM, BY SOME PERMUTATION GROUP

A CONVENIENT APPROACH  ALTERNATIVE TO THE PERMUTATION
VECTORS, IS IN TERMS OF BOOLEAN PERMUTATION MATRICES
 P  UNDER THE RELATIVE PRODUCT "∨.∧", SINCE HERE THE
INVERSE OF  P  IS SIMPLY ITS TRANSPOSE  ⍉P

RECASTING THE AUTOMOBILE EXAMPLE IN THIS FORM WE
FIND, CORRESPONDING TO THE FOUR PERMUTATIONS
      E                 A                 B                 C
1 2 3 4           3 4 2 1           2 1 4 3           4 3 1 2

AND INTRODUCING THE UNIT MATRIX
                  M←(⍳4)∘.=⍳4

THAT THE PERMUTATION MATRICES ARE
      M[;E]             M[;A]             M[;B]             M[;C]
 1 0 0 0           0 0 0 1           0 1 0 0           0 0 1 0
 0 1 0 0           0 0 1 0           1 0 0 0           0 0 0 1
 0 0 1 0           1 0 0 0           0 0 0 1           0 1 0 0
 0 0 0 1           0 1 0 0           0 0 1 0           1 0 0 0

THE GROUP OPERATION IS NOW THE RELATIVE PRODUCT
      M[;B]∨.∧M[;A]                     M[;C]∨.∧M[;B]
 0 0 1 0                           0 0 0 1
 0 0 0 1                           0 0 1 0
 0 1 0 0                           1 0 0 0
 1 0 0 0                           0 1 0 0

WHICH IS ASSOCIATIVE
      M[;C]∨.∧(M[;B]∨.∧M[;A])
 0 1 0 0
 1 0 0 0
 0 0 0 1
 0 0 1 0
      (M[;C]∨.∧M[;B])∨.∧M[;A]
 0 1 0 0
 1 0 0 0
 0 0 0 1
 0 0 1 0

AND COMMUTATIVE
      ∧/,(M[;B]∨.∧M[;A])=M[;A]∨.∧M[;B]
1

THE NEUTRAL STRATEGY  M[;E]  IS CLEARLY THE IDENTITY
ELEMENT  AND EACH ELEMENT HAS A TRANSPOSE OR INVERSE
      M[;⍋A]            ⍉M[;A]            M[;A]∨.∧⍉M[;A]
 0 0 1 0           0 0 1 0           1 0 0 0
 0 0 0 1           0 0 0 1           0 1 0 0
 0 1 0 0           0 1 0 0           0 0 1 0
 1 0 0 0           1 0 0 0           0 0 0 1
```

Figure 24 Boolean matrix representation of the automobile example

	APL notation	Explanation
Cartesian matrix product	*P←S+.×T*	$P_{ij} = \sum_{k=1}^{k=n} S_{ik} \times T_{kj}$
Boolean relative product	*P←S∨.∧T*	$P_{ij} = \bigvee_{k=1}^{k=n} S_{ik} \wedge T_{kj}$

Figure 25. Two basic inner products

symbolic logic represent relations. Thus, considering the two Boolean matrices "*S*" and "*T*" in figure 25 as each a relation, then we have, tracing the general entry, that index "*i*" has the relation "*S*" to index "*k*", and index "*k*" has the relation "*T*" to index "*j*". What the relative product of "*S*" and "*T*" then does, is that it short-circuits the intermediate index "*k*" by establishing that index "*i*" has the compound relation "*P*" to index "*j*". Mathematically, this is no more than invoking the so-called *transitive law*, that if "*i*" is related to "*k*", and "*k*" is related to "*j*", then "*i*" is also related to "*j*". To illustrate, the relative product of *brother* and *father* is *paternal uncle*, and the relative product of *father* and *father* is *paternal grandfather*. In other words, the relative product implements by computation the process of drawing logical conclusions. This explains the popularity that this approach enjoys in modern computer applications.

Returning to figure 24, we may now use the relative product to test by computation that the four strategies constitute the elements of a group. One problem which turns up here, is the question of defining the *inverse* of a Boolean matrix under the relative product. Based on the well known definition that the product of a matrix and its inverse shall be the unit matrix (just like the product of a number and its reciprocal shall be the unit value), R. D. Luce demonstrated in 1952 that the only Boolean matrix which had an inverse in this sense, was a permutation matrix. [49]) He further proved that to find the inverse of a permutation matrix, we merely had to *transpose* (or interchange) its row and column indices. This is interesting, because the structural difference between a Cartesian matrix and its inverse is also such a transposition of row and column indices. Concluding our little digression into digraph theory and Boolean matrix algebra, I must emphasize that the interpretation in general of the transpose of an arbitrary Boolean matrix, is no more than a reversal of the implied relation of an immediate successor to that of

an immediate predecessor. On the digraph, this corresponds to a change of the orientation of all arrows to the opposite orientation.

Cayley's contribution, that a group can be defined without reference to the specific nature of the elements, in more recent times led to the discovery that it was possible to define multiplication tables which only possessed some of the properties associated with the group concept. This in turn carried with it a reformulation of the theory, so that now the group properties are introduced as axioms or postulates which a multiplication table must satisfy in order to be a group. If we confine ourselves to finite groups, these axioms may be given a rather simple formulation in APL, so that they can be tested automatically on the computer terminal. In other words, what we intend to accomplish here is an initial automation of a special kind of "*theorem-proving*" which until the late 1950s was believed to be an act requiring human intelligence.

The group axioms may be formulated in various ways. Figure 26 illustrates, independent of choice of origin, a possible APL formulation of what perhaps is the most straightforward and intuitively simple set of group axioms. [75]) A demonstration of how these APL statements are used in practice on the terminal to actually test a multiplication table, will be given later in the terminal session. Here, it is the underlying mathematical ideas which are of interest.

We will assume that the carrier is a vector "*L*" of distinct elements (either integers or single-character symbols), and that the multiplication table is a square matrix "*T*" of conforming dimensions so that its row and column indices relate to the element ordering in "*L*". The set of four preliminary tests, specified at the top of the figure,

Figure 26. The group axioms.

REQUIREMENT		APL EXPRESSION
LIST L & TABLE T		(1=⍴⍴L)∧2=⍴⍴T
CONFORMING DIMENSIONS		∧/(⍴L)=⍴T
CONFORMING DATA TYPES		(1↑0⍴L)=1↑0⍴T
DISTINCT ELEMENTS		∧/1=+/L∘.=L
POSTULATES	CLOSURE	∧/ T∊L
	ASSOCIATIVITY	[illegible]
	IDENTITY ELEMENT	[illegible]
	INVERSE ELEMENTS	[illegible] [illegible]
	COMMUTATIVITY	∧/ T=⍉T

are intended to verify these assumptions. Thus, we begin by asking if "*L*" is a vector and "*T*" a matrix. We then test whether or not the dimensions conform, the satisfaction of which also implies that "*T*" is a square matrix. For compatibility, we further require that both variables are given the same data representation, either character or numeric. Finally, we have to ensure that "*L*" is specified without repeated elements. Of course, the assumption that the order of the table row and column indices agrees with that of the carrier elements, is not taken care of by these tests since we rely on APL's implicit indexing procedure of arrays. To accommodate such a test, it would be necessary to introduce an additional and explicit indexing of the table.

The satisfaction of these four tests, implies that we have defined in APL a single rule of composition (or binary operation) on a carrier, in a manner amenable to the automatic testing of whether or not this rule possesses certain basic properties in relation to the carrier elements. To describe these properties, we shall find it convenient to introduce five group axioms or postulates, which are listed row-wise below each other in the figure in order of increasing speciality.

It is important to note that, apart from the last axiom on commutativity, the ordering of the axioms is *cumulative*. That is, the introduction of an axiom is only algebraically meaningful if all of the preceding axioms are satisfied. In other words, we successively endow the operation on the set with more and more properties or, as it is called, algebraic structure. Hence, the failure of satisfying an axiom means that, although the operation on the set does not constitute a group, we have found a distinct and important structure. Mathematicians destinguish terminologically between these degrees of distinct structure, so to understand what they are talking about we shall also introduce the appropriate designations. Undoubtedly, these distinct structures were discovered by relating algebraic properties to observations of spatial patterns of symbols in the multiplication table. This geometrical interpretation is of more than explanatory interest. It also provides the basis of particularly simple tests of the axioms.

The axiom of *closure* implies that every element of the multiplication table is also an element of the carrier. The simplest way to test this property is therefore by means of the membership function. A binary operation on a set which satisfies this property, is known as a *groupoid* in the mathematical literature.

The *associativity* of the operation means that all products of any three elements "*X*", "*Y*", and "*Z*" satisfy the condition:

(*X*□*Y*)□*Z* ↔ *X*□(*Y*□*Z*)

Particularizing this statement about scalar tuple products to outer products of the vector "*L*" by itself, we exhaust all possible combinations by the requirement:

(*L*∘.□*L*)∘.□*L* ↔ *L*∘.□(*L*∘.□*L*)

From figure 23 it may be recalled that in principle the multiplication table was defined

T ↔ *L*∘.□*L*

Substituting the content of the two parentheses by this expression, we may rewrite the condition:

T∘.□*L* ↔ *L*∘.□*T*

Introducing a *table look-up* representation of the outer product, we can use indexing to implement this purely abstract formulation:

T[*L*⍳*T*;*L*⍳*L*] ↔ *T*[*L*⍳*L*;*L*⍳*T*]

This expression can be abbreviated further, as shown in the figure, if we use the characteristic identity of the APL indexing notation:

T ↔ *T*[;] ↔ *T* [*L*⍳*L*;*L*⍳*L*]

An algebraic structure satisfying the axioms of closure and associativity, is called a *semigroup*.

To establish that the structure has a unique *identity* or *neutral* element, say "*I*", we require that it (and only it) satisfies, for every element "*X*", the *identity law*

X□*I* ↔ *I*□*X* ↔ *X*

The implication of this law is that exactly one row and the corresponding column in the table "*T*" are replicas of the carrier "*L*". To verify this requirement for the row, say, we introduce the Boolean inner product

T∧.=*L*

the result of which is a vector of the same dimension as the carrier, and with the position of the replica indicated by a "1" and zeroes elsewhere. Using the same idea for the column, we have designed the test so that it actually determines the unique identity element. An algebraic structure meeting the conditions for closure, associativity, and an unique identity element, is designated a *monoid*.

To demonstrate that each element "*X*" of an algebraic structure has an *inverse* element, say "$\underline{X}$", satisfying the *inverse law*,

X□*X* ↔ *X*□*X* ↔ *I*

two conditions must be satisfied. First, the identity element "*I*" must appear exactly once in each row and column of the table, because otherwise there would not be a unique inverse of each element. Secondly, the positions of the identity element

must be symmetrical about the principal diagonal (from upper left to lower right) in order to accomodate both statements of the product in the inverse law. It follows that the entries of the identity element:

$$T\epsilon I$$

will specify a symmetrical permutation matrix of the dimensions of the table. The corresponding test is straightforward since we merely have to invoke the two definitions of a permutation matrix and a symmetrical matrix, respectively. A slightly more compact variation which is illustrated here, is to introduce Luce's theorem, discussed earlier in connection with figure 24. That is, that a permutation matrix is the only Boolean matrix which has an inverse under the relative product, namely its transpose. This fact together with the definition that a symmetrical matrix is equal to its transpose, provide the explanation of the statement of the inverse law in figure 26. With this law satisfied, the inverse elements of those in the carrier "*L*" are determined in the same order in the conforming vector "*L*". If an algebraic structure submits to the inverse law as well as to the previous three laws of closure, associativity, and a unique identity element, it is a *group*.

Finally, *commutativity* of the operation means that the product of any two elements satisfies the *commutative law*

$$X \square Y \leftrightarrow Y \square X$$

Since each corresponding pair of products is located symmetrically with respect to the main diagonal of the multiplication table, all that is required in order to test this law, is to verify whether or not table "*T*" is a symmetrical matrix. It is useful to know that, whatever degree of algebraic structure a multiplication table may possess, there is always the possibility that it may satisfy this law and, hence, be qualified by the adjective *commutative*. Thus, mathematicians speak of commutative groupoids, semigroups, monoids, or groups. The latter, as I mentioned earlier, are also known as *Abelian groups*.

It should perhaps be emphasized that the APL statements of figure 26, merely illustrate one out of many ways in which the group axioms may be implemented. Mathematics, as conceived today, is fundamentally the study of structure, and there is hardly any better educational and more motivating tool for bringing across interest, insight, and understanding into this abstract topic, than to let the student himself explore the notational power and elegance of APL as he proceeds into this area, beginning with a design of his own axiom tests. The notions of a multiplication table and an algebraic structure are at the foundation of applying computers, so it is fortunate that so many professional mathematicians have directed their

attention to the pedagogical problem of bringing down this material to the high-school or gymnasium level, and with so brilliant results.[74] Simultaneously, however, it should be noted that the computer imposes new problems on the mathematical formulation; problems which must be met in the teaching situation. For example, since direct verification of the associative law is considered too laborious, the thorough discussion of this axiom is usually postponed to much later in the course in order to overcome the difficulty by indirect and more sophisticated methods. However, as I shall demonstrate later, it is the kind of brute-force method illustrated here in APL, which is slowly becoming of interest.[75] The reason for this change is far more fundamental than the mere question of easy access to powerful computers. In mathematics, traditionally, we *analyze* given multiplication tables. The problem now facing us, is how to *design* such tables by gradually extending the number of elements in the carrier.

In this conncection, one should be aware that alternative formulations are possible of the axiom system expanded here. For example, in the case of finite groups, the identity and the inverse laws may be combined into a single postulate, demanding *a unique solution for any group equation*. This property is often known as the *possibility of division*. It is verified when each row and column of the multiplication table "*T*" is a permutation of the defining list "*L*". Incidentally, any multiplication table satisfying this last-mentioned requirement is known as a *Latin Square*.[16] Such squares have become a useful technique in the design of statistical experiments.

We have now acquired the necessary insight into the abstract concept of a mathematical group, so that we can understand and appreciate the contribution Klein made to science enunciating his Erlanger Program. Group theory measures the algebraic structure of a binary operation on a set by investigating the regularities or patterns of the associated multiplication table. Depending upon application, a multiplication table may be given a variety of *representations*, so that one and the same pattern can be masquerading in different disguises. However, independent of the accidental representation, group theory enables us to identify and compare these patterns, as well as to determine their abstract properties. But group theory also generalizes our more naive conception of a multiplication table by making us aware of the fundamental similarity between, say, the table for addition of natural numbers and the table of strategies for changing the tires in our automobile example. Indeed, group theory provides the most fundamental description of what happens when one kind of mathematical operation is performed on different elements, or when different operations are successively performed on a single element.

In his Erlanger Program, Klein focused on the last-mentioned interpretation when he proposed to use group theory for "*bringing formally into evidence*" the

independence of geometrical properties upon the arbitrary choice of a coordinate system. His bright idea was that, for each geometry, there would exist a set of characteristic transformations of the manifold or abstract space which, performed successively, would leave invariant the geometrical properties, usually referred to today as the *symmetries* of the manifold. In other words, the multiplication table of this set of transformations would form a group. Since the pattern of this group would reflect the structure of the particular geometry under investigation, it could be compared with the group pattern of other geometries. To provide a scale for comparing geometries in terms of their group of characteristic transformations, it was natural to introduce the set of abstract groups derived in group theory. From there it was but a small step to visualize that measurement of invariance could be undertaken in general by comparison with a scale of abstract groups. Thus, when Klein published a slightly extended version of his program some twenty-one years after he first enunciated it, he said in a footnote: 50)

> *"Indeed, from my present standpoint I would have made larger changes in the Program. ... I would have tried to bring out all applications of the theory of manifolds, not only those of geometry but equally well those of mechanics and mathematical physics"*

Clearly, what Klein recognized here, was that abstract groups provided the mathematical tool for the formal study of regularities or patterns in the behaviour of natural or man-made systems.

To appreciate how epoch-making Klein's idea was at the time, it should be made clear that, when Klein entered the scene, the different geometries could not be compared. They were all derived axiomatically as each a separate theory like Euclid's geometry, and there existed no common principle from which they could be derived. Simultaneously, however, the number of different geometries was rapidly multiplying. Thus, apart from the non-Euclidean geometries of Gauss, Bolyai, and Lobatchevsky, the work on affine and, in particular, projective geometry had progressed significantly due to the efforts of Möbius, von Staudt, and Cayley. Further, as Klein pointed out in his Program, other kinds of geometry, such as inversive geometry (die Geometrie der reciproken Radien) and algebraic geometry (die Geometrie der rationalen Umformungen) had emerged

To introduce the basic idea, Klein opened the formulation of his Program by considering *"an example of a group of transformations ... given by the totality of motions (considering each motion as an operation on space in its entirety)"*. Then, after having extended the example considering reflections and other sense-reversing similarities, he continued: 50)

> *"The aggregate of all these transformations we shall denote the* principal group *[Hauptgruppe] of spatial changes, geometrical properties are not changed by the transformations of the principal group. Conversely one might say: geometrical properties are characterized by their invariance under the principal group of transformations Because, if one considers space as motionless etc., as a rigid manifold, then each figure has an individual interest; still, of the properties it has as an individual, it is in fact only the geometrical ones which are preserved by the changes of the principal group.*
>
> *. Let us now erase this mental image as mathematically insignificant and consider in space only a multiply extended manifold, and also, in that we maintain the usual conception of points as spatial elements, one which is threefold extended. By analogy to the conventional spatial transformations we will speak of transformations of the manifold; they, too, form groups. Only now it is no more as in conventional space, that one group is more significant than the others; every group is of equal interest. Hence, the following extended problem arises as a generalization of geometry.*
>
> *Let there be given a manifold and an associated group of transformations; one should investigate the image of the manifold with respect to those properties which are not changed by the group of transformations. By analogy to the modern way of expression, which is usually applied only to one distinct group, the group of all linear transformations, one could also say:*
>
> *Given a manifold and an associated group of transformations, the theory of invariants of this group is to be developed"*

Hence, as Klein formulated it, his basic idea was that each geometry can be characterized by a mathematical group of transformations and, conversely, that a geometry is really concerned with invariants under this group. Moreover, as he continued his explanation, because some groups contain others as subgroups, some geometries will embrace others. That is, a subgroup of the transformation group of some geometry will define a subgeometry so that all theorems of the original geometry will continue to be theorems in the subgeometry. Further, since the transformation group of a geometry may contain more than one subgroup, it may be possible to define alternative subgeometries of a given geometry. Accordingly, rather than a scale in the usual sense, we see that the abstract groups form a classification scheme branching out like a tree. At the root of this tree, we find the most general group, embracing all other groups. This is the group of all permutations, the so-called symmetrical group.

Group theory is a powerful tool, so the success of the Erlanger Program in physics and chemistry perhaps justified Klein's friend Sophus Lie in his enthusiastical query: *"What are the phenomena of the physical and material universe but the transformations of an enormous group, of which the laws of nature are the invariants?"* Though, as any other tool, group theory has its limitations. In many applications, for example, it is necessary and useful to deal with algebraic structures which violate one or more of the group axioms. For instance, we quite often find that an inverse does

not exist. To cope with such situations, we may accept a generalized form of the Erlanger Program, admitting algebraic structures such as monoids or semigroups. However, in the area of cryptography this is of less interest, since to be meaningful encipherment and decipherment must be inverse operation

2.10 The Scaling of Data

Euripides, the famous author of *Medea, Iphigenia in Aulis,* and other classical Greek tragedies from about 450 B. C., was quoted by Pliny the Younger [76]) for a statement of profound insight: *"Tell me what company thou keepest, and I'll tell thee what thou art"* In fact, had it not been for its implication of moral judgment, this sentence would make a nice motto of scientific explanation.

The scientific meaning of a thing is its observed relationships with other things. The purpose of introducing a mathematical description of such relationships is to get away from subjective ideas of what things are. But equally important, it is a means, as the Nobel Price winner in physics, P. W. Bridgman, once expressed it, for reducing a situation to elements with which we are so familiar that we accept them as a matter of course, so that our curiosity rests. [77])

In 1957, in a fascinating book dedicated *"to my dog Pym,"* Colin Cherry presented this idea in a nutshell by illustrating, how a "nonsense" sentence preserves its form under translation from one language to another: [78])

English: *The ventious crapets pounted raditally*
German: *Die wenten Krapetten ponteten raditat.*
French: *Les crapêt ventieux pontaient raditallement.*
Danish: *De ventiøse krapetter ponterede raditalt*

Evidently, we have here different language representations of only a single abstract relationship which forms a systematically composed body of words. For the sake of argument, let us call the common grammatical structure of these nonsense sentences, the "Indo-European form". *Syntax* is the abstract way of describing such a form "mathematically" disregarding all but the mere arrangement which characterizes the sequence or word-combination, and the specific word properties derived from a grammatical classification of words. To admit different word arrangements, the sentence structure is subdivided into *phrases*, which are two or more words in sequence, forming a syntactic unit less complicated than the sequence. The word-classification is hierarchical. Most fundamental are the *substantives* (Latin: self-existent) and the *verbs* (Latin: words). To modify these two classes we adjoin each a class of qualifiers, namely *adjectives* (Latin: attributed) and *adverbs* (Latin: added word), respectively. Based on this classification, we may now identify certain meaningful word sequences or phrases such as the *predicate* (Latin: to proclaim). Thus,

by continuing this approach we can build up a formal or syntactic description of a sentence structure, "the Indo-European form", which sentences in English, German, French, or Danish will satisfy. Hence, instead of considering the sentence structure for each particular language, we can concentrate on the abstract form which is preserved as an invariant under translation from one language to another. In other words, we may conceive sentences in the various languages as different representations of the same abstract form. Chinese dialects, however, do not satisfy this particular abstract form; so here we will have to start afresh, establishing a corresponding invariant sentence-form with the different dialects as its representations. The two different sentence-forms, the "Indo-European" and the "Chinese", may now be used in the investigation of sentences formulated in known or unknown languages.

Of course, all this is really a fictitious illustration. The richness and fantasy of language, explored by poets and others who have the command of it, often lie in its ambiguity or violation of grammatical rules. Still, by bending the truth we have produced here a simple picture which by analogy suggests two important concepts to look for in the discussion to be undertaken now. In this respect, we shall find it useful to imagine for each language a set of nonsense sentences which may serve as a "scale" for all genuine sentences in the language, by virtue of the fact that this set contains one example, a "standard", of each structually different kind of sentence. These "scales", one for each language, are therefore the different representations of a common "scale-form", exemplified above by the "Indo-European form". The interplay between scales and scale-forms, is the picture we should keep in mind.

Data (singular: *datum*) is Latin for "that which is given", namely the facts used to draw a conclusion or make a decision. It is accepted usage of the term that the facts are given interchangeably by: assumption, measurement, or logical derivation from other facts. It follows, to be consistent, that at least in some form, data will satisfy the generally acknowledged properties of measurements. Hence, to arrive at a scientific explanation of data and the way in which they are recorded, let us leap right into that part of the general theory on measurements which pertains to the abstract structure of their symbolic representations. Hereby, we not only skip all physical aspects of the measurement process itself, but also the associated theoretical interpretations which after Bridgman came to be known as the *operational viewpoint.* [79]) Since the word "operational" refers to the operations or manipulations of actually performing the measurement, the interpretation to be adopted here has been designated the *symbolic viewpoint* by virtue of the fact that it applies to the symbolic recording of measurements.

The generally accepted meaning of the term measurement is the assignment of numbers to represent properties. In principle, the assignment is by comparison

according to some consistent convention or direction, which in general may be denoted a *rule of comparison*. The "standard property" with which we compare, is known as a *measurement scale*, because it prescribes what numbers to assign. Since the choice of "standard property" may vary, as determined by empirical considerations and preferences, a property may be measured on different scales. These scales will be in one-to-one correspondence with each other, so that a scale *conversion* is always possible. We shall designate the set of algebraic properties, which are preserved under such scale conversions, a *scale-form*. Hence, from a mathematical point of view the different scales are but different algebraic representations of one and the same invariant form.

For centuries it was assumed that measurable properties were quantities, so that the assigned numbers represented magnitudes. In other words, to be acceptable as measurement, it should be meaningful to apply the concept of addition to the assigned numbers. Thus, a committee of the British Association for the Advancement of Science, made up of mathematicians, physicists, and psychologists, sat from 1932 to 1939 without being able to reach an agreement on, whether or not what psychologists purported to be a measure of human sensation, was at all a meaningful application of the term. As it came out in the final report in 1940, the crux of the matter was that psychologists, assigning numbers to qualities rather than to quantities, had dared to describe this as measurement.

A distinguished member of the committee supporting the novel view, was the physicist Norman Robert Campbell who already by 1919 had arrived at a very general and fundamental conception of measurement. [80]) Thus, he accepted as a genuine measurement Mohs' well known scale of hardness which orders minerals according to whether or not they can scratch each other. Likewise, he was touching upon the problem that numbers "*provide an inexhaustible series of names* [for] *objects, such as soldiers or telephones, which have no natural order*". Another important observation of his was that the measurement of a point in time, say 3 o'clock, differed basically from that of a period of time such as the duration of 3 hours. These deviations from the hitherto accepted notion of measurement led him to the important idea, that measurement is not an assignment of numbers implying the validity of all the algebraic properties of this concept like that of addition, but an assignment of number symbols or representations, the so-called *numerals*, devoid of any algebraic properties but those explicitly ascribed to them. As used in the term Roman numerals, such number symbols could be letters as well as figures, and in fact he compared Mohs' hardness scale with an alphabet.

Campbell's work inspired the psycho-physicist S. S. Stevens of Harvard University to the formulation in 1941 of a fundamental classification of measurement in terms of the four invariant scale-forms shown in figure 27. This contribution was

Scale form	Basic empirical operation	Algebraic rule of classification	Algebraic structure: Binary relations	Algebraic structure: Binary operations	Group
Nominal	Determination of equality	=	=		Symmetric
Ordinal	Determination of rank-order	<	=<		Monotonic
Interval	Determination of the equality of intervals or of differences	−	=<	+	Affine $x'=ax+b$ $a>0$
Ratio	Determination of the equality of ratios	+	=<	+ ×	Similarity $x'=ax$ $a>0$

Figure 27. A classification of measurement by scale-forms.

published in 1946 in a now classic article. [80]) Although it is not mentioned explicitly in this article, Stevens' classification implemented the Erlanger Program for measurements. Further, it so happens that the defining four groups are well-ordered with respect to being subgroups of each other. The reason for this, as we shall shortly see, is that the algebraic structure of the scale-forms is cumulative. In fact, there is a striking resemblance between the accumulation of structure by the scale-forms and that by the group axioms. It seems pretty certain that physics was Stevens' source of inspiration. [81]) A footnote to his article, casting an interesting sidelight in this respect, is the following

> "*A classification essentially equivalent to that contained in this table* [see figure 27] *was presented before the International Congress for the Unity of Science, September 1941. The writer is indebted to the late Prof. G. D. Birkhoff for a stimulating discussion which led to the completion of the table in essentially its present form*".

George D. Birkhoff, the mathematical physicist referred to here by Stevens, pioneered the use of the group-theoretical approach to mechanics in a now classical work from 1927. [82]) In this work, rather characteristically, Birkhoff invented names of his own, such as the "formal group" and the "extended group", for the mathematical groups under consideration. Perhaps he also suggested the name: the "isotonic" group, originally adopted by Stevens in connection with the definition of the ordinal scale-form.

It is remarkable to observe that this idea of using group theory to classify scales of measurements, was proposed independently about the same time, namely in 1945, by John von Neumann and Oskar Morgenstern in their celebrated book on Game Theory. [83]) It was in this connection that they introduced the now classic terminology in economics of defining measurements "*up to*" a system of such-and-such transformations. Thus, they said:

> "*Passage from one of these correlations* [read: scale] *to another amounts to a* transformation *of the numerical data describing the physical quantities. We then say that the physical quantities in question are described by numbers* up to *that system of transformations. The mathematical name of such transformation systems is* groups

Later in the book, they disclose that their purpose is to take advantage of the many abstract symmetries; and to capture the imagination of their readers, they explicitly refer to Weyl's book on symmetry. Although the words: scale or scale-form do not appear in their discussion, they clearly identify by their group-theoretical designations that measurements fall in the four classes also identified by Stevens, and they illustrate each of these classes by examples such as Mohs' scale of hardness. Also, their choice of the terminology "*up to*", is clearly intended to suggest the cumulative nature of the scale-forms

The columns of the table in figure 27 list different properties of the four scale-forms given one in each row. The last column specifies the defining property, namely the *group of transformations* under which the scale-form remains invariant The designations of the groups adopted here, originate in the mathematical literature, and are basically those given by von Neumann and Morgenstern. Combining the exposition of these two authors with that of Stevens, we may explain the classification of scale-forms in relation to the group properties as follows, considering one row at a time

A ordinal scale admits any permutation or one-to-one substitution of the assigned numerals since, basically, the scale-form partitions the measurements of the observable property into *equivalence classes*. The scale-form for N classes is characterized by the so-called *symmetric group* of degree N. That is, the group of all permutations of N elements.

An *ordinal scale* introduces a rank-ordering that can be transformed by any *monotonic function* whether increasing or decreasing. In economic parlance, we say that the observable quality may be measured up to any monotone transformation. The defining group was originally designated the *isotonic group*, as mentioned previously.

An *interval scale* defines measurements of an observable quality up to any positive linear transformation or (with a loan from geometry) *affine transformation*, involving addition of any constant and multiplication by any positive constant. The adding of a constant introduces a new reference or zero point, whereas the multiplication by a factor changes the unit.

A *ratio scale* specifies measurements of an observable quality up to any positive linear transformation based on multiplication by any positive constant. Thus, the unit may change, but the reference or zero point is fixed or absolute. The name of the group originates in geometry where *similarity* is a one-to-one transformation that multiplies all lengths or distances by a positive factor.

From this description of the rows of the table, let us turn to a discussion of the columns beginning with the first. In 1959, in a personal report on the nature of things, Percy Bridgman remarked that "*the criterion of successful description* [read measurement] ... *is that we shall be able to reproduce it, or at least recognize it when it recurs*". [77]) Put into logical terms, this basically means that, to be classified as a successful observation, the underlying empirical operation must satisfy what is known as the transitive law, explained earlier.

Only experience can decide whether this law is satisfied, or the empirical observations are merely accidental. But note, the decision to accept, is a question of confidence. Contrary to common opinion, science does not prove anything about real-world relationships All it can do, is to disprove assumptions about such relationships In principle, nothing is easier All one has to do is to discover a case where the relationship fails. In practice, it is far more difficult. Just imagine that it had to be done consulting tables exhaustively cataloguing all concrete cases. Hence, to overcome this problem, science has devised an alternative organization which in some optimum way makes the accumulated experiences "*vulnerable to disproof*", to quote Sir Karl Popper. [84]) This is the logically consistent theory or model, because this construction is testable in the sense that it can be falsified Among other things, this implies, as pointed out by Popper, that "*the simplicity of a theory is connected with its falsifiability, i.e. with the ease of its elimination*". By clothing a theory or a model in the formal garment of mathematics, we make it simpler simultaneously with preparing it for easy and fail-safe manipulation. But the implication of this step goes beyond that. As Feynman emphasized it, "*mathematics is* not *just another language. Mathematics is a language plus reasoning; it is like a language*

plus logic. Mathematics is a tool for reasoning" [68]) Theory, therefore, is not only what makes science testable, it is also what makes it teachable. Yet, do not be mistaken. Theoretical results are conclusions drawn from centuries of experiments. They are not conclusions deduced logically from some philosophical first principles.

The algebraic properties ascribed to the measurements, constitute the platform of a theory or model. In no way can it logically expand beyond the boundaries set here. The transitive law, in this connection, determines whether or not conclusions can be deduced. At the outset, the law is invoked in the measurement process itself by the rule of comparison. The law is the basis for drawing conclusions from the introduction of a "standard property" as a scale. Thus, if two separate properties stand in the same relation to the "standard property", we deduce logically by the transitive law that they stand in the same relation to each other. This illustrates the meaning of Feynman's statement about the double role of mathematics, as a language, and as a tool of reasoning.

Equality and order are the two relations in terms of which we may express the transitive law. Equality alone provides the most unrestricted assignment of numerals, namely the labelling of items. Football players are an often quoted example. With no loss of meaning, they could as well be labelled with APL symbols of operations, provided that no two players are assigned the same symbol. In general, measurement on a nominal scale is based on some empirical operation for identifying, classifying, or discriminating items according to a particular property. Determination of rank-order implies that the empirical operation pertaining to an ordinal scale, should accomodate both equality and order. The meaning of the scale concept is that a comparison can be made without exception. Therefore, we cannot discard the relationship of equality. The description of decision-making in economic utility theory in terms of indifferences and preferences, explicitly emphasizes this fact. Normally, however, the two relationships are combined into one, a so-called partial order, well-known from the assignment of street-numbers. With the interval scale, we come to a form that is "quantitative" in the ordinary sense of the word. The characteristic feature is that it is empirically meaningful to compare intervals or differences. Temperatures, dates, and similar kinds of measurements where we can arbitrarily select a "unit" and a "zero point", constitute the properties measured here. Of course, in addition to equality, we will also have a relationship of "greater" or "less". Note, that although the assigned numerals submit to the rule of addition (actually subtraction), it is meaningless to inquire about ratios; for example, to calculate that the year 1984 is 1.984 larger than the year 1000. In fact, the ratio scale is the only scale where it is meaningful to ascribe all the algebraic properties of number to the assigned numerals.

This leads us to the column of the table which describes the cumulative property with respect to the *algebraic structure* of all four scale-forms. The implication of this property in relation to the partition into binary relations and binary operations, is that all scale-forms will exhibit the structure of a binary relation, whereas only two will admit the additional structure of a binary real number operation. In particular, any scale-form will add a new algebraic property to those of the scale-form listed above it. Thus, in the process of developing the different scale-forms more and more algebraic properties are introduced. Of course, at the same time as the algebraic structure is endowed with more properties, it also becomes more specialized.

This specialization is reflected in the *group-theoretical structure* of the four scale-forms defined in the last column. To be sure, each mathematical group defining a scale-form is a subgroup of the group listed above it in the table. To illustrate, let us consider the nominal scale-form which represents empirical information in the algebraic form of an equivalence relation. Thus, the implication of this scale-form is that measurements of an observable property are assigned the same numeral only if they belong to the same equivalence class, and that no measurements belonging to any other class are assigned that numeral. It follows, that this property is preserved under any permutation among the classes of the assigned numerals. It is for this reason that the defining group is the *symmetric group*, or the group of all permutations. The general nature of this group derives from the fact mentioned earlier that the entire theory of finite groups can be developed indirectly as a branch of the theory of permutations. Another illustration relates to the *affine group* defining the interval scale-form. This group is also known as the *"extended" similarity group*, because it consists of all affine transformations in which the change of unit is a similarity transformation. Hence, a subgroup of this group is the *similarity group* defining the ratio scale-form. A practical consequence of importance, is the fact that differences between measurements on an interval scale are measured on a ratio scale. Thus, while it was meaningless to introduce the ratio between two calendar years, it is indeed meaningful to compute the ratio between two time-spans, each defined as the difference between one year and another.

The physical reality of the world we live in, has made us all familiar with measurements on interval and ratio scales. Thus, we can all agree that dates on a calendar, temperatures in Celsius or Fahrenheit, positions in a coordinate system, and potentials of any kind, are measured on interval scales. In contradistinction, we find it far more difficult to identify measurements on nominal and ordinal scales. It is not because such measurements are rare, since truly they are abundant. Rather, it is because we do not recognize their use as measurements. Telephone and street numbers are well-known concepts in our daily life, but in spite of their usefulness we hesitate to accept them as measurements though their importance

stems from the fact that, usually, telephone numbers are defined on a nominal scale and street numbers on an ordinal scale

A widely accepted misconception in this connection, seems to be that measurements on nominal and ordinal scales cannot be operated on like measurements on interval and ratio scales. Definitely, the binary number operations of addition and multiplication are not defined for measurements on nominal and ordinal scales but, as we have illustrated in figures 23-25, corresponding Boolean or other equally meaningful operations exist which can be introduced instead, whenever it is deemed profitable. Of course, it is here assumed that any such operation submits to the defining group of the scale-form in question

It would be wrong to end our discussion of scale-forms without considering those situations where we may find it difficult to ascertain the basic empirical operation defining the scale-form. In such cases, as suggested by Stevens, it may be useful to proceed in the following manner based on the dual cumulative properties of the last two columns

Assuming that the measurements are assigned numerals representing the common number system, we simply ask ourselves: In which ways can we transform the measured values and still have them serve all the functions originally fulfilled? We know that the values on any ratio scale can be multiplied by a constant which changes the size of the unit. If, in addition, a constant can be added (or a new zero point chosen), it is proof positive that we are not concerned with a ratio scale. Then, if the purpose of the scale is still served when its values are squared or cubed, it is not even an interval scale. Finally, if any two values may be interchanged at will, the ordinal scale is ruled out, and the nominal scale is the sole remaining possibility.

What we have seen here, is that the Erlanger Program provides a classification of measurements by scale-forms. Thus, paraphrasing Klein, we may say:

Measurements are classified according to the group of transformations which leaves the empirically given scale-form invariant.

Hence, whatever the actual operations of observation are, that which gives empirical meaning to measurement, is their scale-form. It follows, that preserving the scale-form algebraically is tantamount to preserving the empirical information. This is the essence of the interpretation of measurements by the symbolic viewpoint.

However, there is one important point which we have glossed over here, though we have discussed it in some detail earlier; that is the fact that measurements of properties make sense only if we know the properties of what. The definition of measurement, which originates in the systematic and elaborate analyses of the subject by Campbell and Stevens, takes this point into consideration

Measurement is
the Assignment of Numerals
to Observable Properties
of Objects or Events
According to Rule.

In his contribution from 1959, Bridgman remarked, referring explicitly to Campbell and Stevens, that objects or events might be called "*situations*" in general An alternative term which has also been used in the literature, is "*entities*". Rather than terminology, however, what is important here, is to clarify the different ingredients of the definition, specified each in a line. Previously it has been emphasized that measurement is "the assignment of numerals"; that this assignment was "to observable properties"; and that the assignment took place "according to a rule", namely a rule of comparison. Therefore, the new point brought out explicitly by this definition, is that we are measuring properties "of objects or events"

But if a measurement is merely represented by the "assigned numeral", the measurement itself cannot simultaneously identify the "object or event". Indeed, merely to place a label on the "object or event", is another measurement performed at least on a nominal scale. Continuing this process of applying the definition of measurement, we are caught in an infinite recursion. The way out to end this loop appears to be, as I interpret Popper, that at some step the objects or events are identified purely conceptually. Thus, he says: [34]) "*Observations, and even more so observation statements and statements of experimental results, are always* interpretations *of the facts observed; ... they are interpretations in the light of theories*". In other words, we must ultimately take something for given. This is the crux of the matter; because to take into account the representation of what is involved in the definition of a measurement, is to leave the realm of measurement. In the marriage of measurement and data, this is where their ways part.

Until this point of our discussion, it has been assumed that data represent the "observable properties" given by measurements. That is, data are numerals which preserve their status as facts under the group of transformations of the defining scale-form. Generalization of this interpretation of the data concept to accomodate the "objects or events" in the definition of measurement, requires that we consider relationships between data or, as we shall call it, *data structures*. Thus, data are related to each other by a context-dependent algebraic structure, which is introduced in addition to the numeral representing the measurement. Generally, therefore, the basic difference between data and measurements is that the former are structured, whereas the latter are not.

There is another difference, however, which we shall also have to take into account. This is the usage of the data concept to describe facts logically derived

from other facts. It might be thought, perhaps, that this situation is already taken care of in the definition of the scale-form. Still, the logical derivation of facts does not necessarily mean that the original facts can be deduced from the derived facts. Knowing a sum is not the same as knowing its component figures. This implies that the logical derivation may involve the use of transformations for which no inverse exists. Hence, algebraic structures more general than groups may be invoked to produce new representations that are but subsets of the original facts.

The representation of data structures by finite arrays is a familiar concept from earlier discussions, so all we need to say at this point is that to achieve well-ordering, the axes must define ordinal scale measurements or data. Yet, since the defining group of transformations for this scale-form is a subgroup of the symmetric group, it is not only meaningful but often also very convenient to discuss many properties of the axes from the viewpoint of nominal scale measurements. Indeed, any algebraic property which can be proved true under the nominal scale will also be true under the ordinal scale.

The first to undertake a consistent study of the notation and algebraic-geometrical properties of *finite, rectangular data-arrays* or, as he called it, "*n-way matrices*", seems to be Gabriel Kron. Extending the content of a couple of articles published 1935 in the General Electric Review, he presented his ideas in the now famous book "*Tensor Analysis of Networks*", from 1939. [65]) Disturbed by the fact that each small problem area in electric power engineering called for some new, often ingenious approach, he declared it the aim of this book "*to introduce mass production into the analysis and synthesis of engineering problems*", emphasizing that "*what is needed for the unified point of view is not additional mathematics, but 'organization' of already employed mathematics*". Indeed, with remarkable foresight he undertook to develop a unified theory which "*facilitates the more systematic use of calculating machines* ...[enabling] *the engineer to delegate a large part of his work to computers*", meaning of course: human computers.

To mechanize the reasoning process and minimize the work in solving problems, Kron adopted from physics the tensor approach promoted by Einstein and others. This approach Kron extended with a new representation of the tensor components as *n*-way matrices or rectangular arrays as a labour-saving device. Thus, he said:

> "*No textbook or publication on tensor analysis employs n-way matrices as a stepping stone to introduce this new method of reasoning. The textbooks simply use expressions such as a 'set of 2³ quantities', without arranging them into a cube with 2 rows, columns, and layers, merely writing the eight quantities in a row side by side. However, the experience in working out numerous engineering problems with this new method of reasoning has led to a systematic use of rows, squares, and cubes in actual calculations which is also employed in this volume. But their use has little to do with tensor analysis; it only facilitates its presentation and application*".

By this invention, Kron clearly preceded APL in adopting rectangular arrays as the fundamental data-structure. Further, to represent the components of his so-called "multiple tensors", Kron even had to introduce *nested rectangular arrays*, for example a table, each element of which is a triple (list), each element of which is again a table. It is thought-provoking that such nested arrays have only recently been admitted into extended versions of APL. In fact, on the point of subdivision or nesting, Kron visualized that, in a theoretical sense, this process may be continued indefinitely

> "*This successive subdivision of a tensor may be continued indefinitely as the complexity of the problem increases, forming in general 'multiply compound tensors' of any complexity, in which the various subdivisions may contain unequal number of component tensors and also may be tensors or geometric objects or n-matrices in any combination*"

As anyone might convince himself, comparing APL with the discussion of data-structures in Kron's publications, Kron pioneered a path of ideas later followed by the originators of APL. [65]) A revealing detail in this respect, may be to compare the print-out in APL of an *N*-dimensional array in terms of two-dimensional matrices (tables) with Kron's remark: "*The breaking up of n-matrices into 2-matrices and representing them so on paper was found by experience to be the most practical procedure for quick or routine solution of engineering problems*".

For Kron with his background in physics, engineering measurements, to be acceptable as such, had to be defined on interval or ratio scale-forms. Still, with uncanny intuition he realized that it should be possible to treat the data arrays defined by the objects or events, separated from the measurements of the observable properties. In fact, he visualized that the data arrays, as geometrical forms void of the entries representing the measured observable properties, must have certain invariant properties. Yet, in the context of his tensorial approach based on the observable properties, only the tensors but not their component arrays, were preserved invariantly under the defining group of transformation. Therefore, to capture the invariance of the component arrays or, as we would say today, the data-structures, he introduced a set of heuristic rules of formulation which he called. "*Generalization Postulates*".

Kron's choice of name caused quite a debate and, as I have mentioned earlier, was certainly frowned upon at the time. Few acknowledged the importance of considering the invariance of form of data-structures "*in order to reduce to a few routine standardized steps the mental labor needed to formulate the large variety of engineering problems*".

The engineering profession in those pre-computer days did not take heed of Kron's ideas, and they found his discussion of invariance of no practical importance. Perhaps, Kron was not without blame either. An anecdote which I have reason to believe true, will illustrate this.

In the late fourties or early fifties, Kron was presenting his ideas at a section meeting in, what was called at that time, the American Institute of Electrical Engineers. To make his point, irritated by what he considered *"stupid questions"*, Kron started hammering the chalk into the blackboard which was placed on a tripod. Suddenly, the blackboard collapsed with an enormous bang. Kron was stunned, but only for a moment. He then turned around towards his audience, crying: *"So powerful are my methods!"*, and walked right out of the room.

Apparently, the engineers were "stupid"; for they were not convinced. Their attitude resembled that of the late nineteenth century British physicists, reflected in Tait's remark of Cayley: [22] *"Is it not a shame that such an outstanding man puts his ability to such entirely useless questions"*. Had Babbage lived, Kron might have found more sympathy there. Thus, in a letter published 1822 in Brewster's Journal of Science, Babbage said about the connection between an important mechanical improvement of his Difference Engine and some *"remote inquiries in mathematics* [that it] *may furnish a lesson to those who are rashly inclined to undervalue the more recondite speculations of pure analysis, from an erroneous idea of their inapplicability to practical matters"*. [20]

The implementation of APL on the computer puts the question of invariance in an entirely new perspective. From the early discussion of the permanence of form by Babbage and his friends to the precise formulation of algebraic invariance by Cayley, Sylvester, Klein, and other mathematicians, the development of the concept belonged solely to the history of modern abstract algebra. The authority of Einstein's genius convinced physicists and other mathematically well-trained scientists that it was a theoretical tool of unrivalled possibilities. Later again, Kron's contribution slowly began to influence the thinking of engineering scientists. What was needed, however, to put the ideas of invariance and structure in use among practitioners over a broad field of applications, was a new tool demonstrating the power of this approach in the solution of real-life problems. The advent of APL announced this era

Let me focus on two properties of APL which in this respect are of principal interest, namely its organization of data in arrays, and its powerful operations for dealing with such arrays as units.

The poorest way of dealing with data is to consider them one by one. This is a formulation technique going against the lesson of modern algebra. To perceive and use the algebraic structure, we must organize data into collections and deal

with them from this overall point of view. Indeed, it is only when data are thus structured that we can identify invariances and take advantage of our highschool or gymnasium knowledge of algebra in dealing with them. Apart from certain macro-programming languages used by small groups of specialists, APL was the first computer language to implement this conception of data. The importance hereof, is that it creates habits of formulations which, when properly directed, focus the attention on the economy of thinking that is the trade-mark of algebra.

Augustus de Morgan, Babbage's mathematical friend who gave name to two important laws of logic, published his *Syllabus of a Proposed System of Logic* in 1860. A thought-provoking quotation from this book is the following: [21]

> *"I end with a word on the new symbols which I have employed. Most writers on logic strongly object to all symbols ... I should advise the reader not to make up his mind on this point until he has well weighed two facts which nobody disputes, both separately and in connexion. First, logic is the only science which has made no progress since the revival of letters; secondly, logic is the only science which has produced no growth of symbols"*.

In this spirit, the lasting contribution of the APL notation is its new view on the question of what constitutes an explicit notation. Of course, no mathematician would hesitate to introduce and use symbols to denote whatever operation he invented; but for the average user there is a built-in barrier in this respect. Operations are to him *plus*, *minus*, etc., as he was taught in mathematics. Beyond that, he conceives them as procedures which must be thought about step-wise. Experience with APL removes this barrier and opens a door towards thinking mathematically.

Naturally, there is a trade-off as the number of symbols multiply. Beyond that, except for the initiated, we will have to write out the names of the operations instead of symbols in order to remember them. Gotlob Frege, the famous logician of the University of Jena whose work was a constant inspiration to Whitehead and Russell, suffered an early neglect due to, what has been called, his *"repulsive symbolism"*. Thus, he himself admitted in a later paper from 1915: [24]

> *"Even the first impression must frighten people away: unknown signs, pages of nothing but strange-looking formulas. It is for that reason, that I turned at times toward other subjects"*.

However, if we consider the symbols of the operations in conventional APL, it is a common experience that they are readily grasped, used, and remembered

As it literally stands for, APL is a programming language. It has powerful and excellent facilities for implementing mathematical models based on data arrays, but

it does not itself constitute a mathematical theory of data. It is an operational notation, as proposed originally by Iverson. As such, it could of course thrive on a theory of data, because a theory could direct the way we teach it, use it, and think about it. This brings us to the question of a mathematical theory of data arrays.

Through the centuries, we have traced the evolution of the abstract ideas which underlie our conception of data arrays and the operations on them. We have built up a fond of knowledge on what constitutes a theory of data arrays and how it could be formally established. In particular, we have seen that, what we have called *array theory*, is a finite geometry whose characteristic properties may be described by algebraic invariants in the sense of the Erlanger Program. By analogy to the discussion on the various geometries alternative to Euclidean geometry, we are further aware of the theoretical possibility that array theory may develop into a class of different geometries, depending upon how the founding set of axioms is specified.

The connectivity or binding property of this class of geometries is well-ordering, just as it is distance for the class of Euclidean and Non-Euclidean geometries. It is important to note here the restriction that we are only considering finite arrays or manifolds, because only *a finite manifold can always be made well-ordered; an infinite, not necessarily so.*

Hence, even in the case that a finite manifold submits to a partial order, so that from this point of view it contains incomparable subsets of points; it can be well-ordered, simply by enumerating its points against a sequence of natural numbers. In a set-theoretical sense, a partial order is determined by the operation called *inclusion*. That is, some sets can be compared because they are included in each other; others cannot because they are disjoint or separated. Keeping this picture in mind, we see why the assumption of a finiteness was crucial to the specification of array theory as a geometry (or class of geometries): in figure 20. In practice, if we think about it, it is this assumption that permits us to compare "incomparable elements" in hierarchical (tree-like) structures by introducing level codes or similar means of providing well-ordering. In the same way, this led us to the fundamental invariance of an array under shape transformations.

Over the past 15-20 years, Trenchard More of the IBM Cambridge scientific Center has developed an algebra, called *Array Theory*, which is the study of the nested rectangular array as a mathematical model of data. This contribution establishes that there are, to quote More, "*laws of data*" governed by equations that arise from the geometrical properties of dimensionality and nesting. In a fascinating account, published 1981 and humbly entitled, "*Notes on the Diagrams, Logic and Operations of Array Theory*", More has presented a survey of his theory, tracing the basic ideas back to Cantor's work on set theory and the ensuing contributions to

mathematical logic by men such as Frege, Zermelo, Fraenkel, and Skolem. [87]) In the establishment of this theory of data, More has worked by analogy to the axiom-set of the Zermelo-Fraenkel set theory so far as possible, introducing only such changes and additions that were necessary to accomodate the notions of shape and dimensionality. The impressive fact is that he had thereby created a geometry of data in the spirit of Euclid. [88])

It is well known that, in whatever programming language, we may program our way around the special cases as they are recognized and the particular problems involved are identified. Still, and this is perhaps the major motivation behind the development of Array Theory, it would be far more desirable to have a unified theory of data for dealing with all individual cases according to a few principles of generally established validity. Thus, More said,

> *"The difficulty of reasoning about special cases in terms of general principles places a premium on developing an algebra of operations, discovering identities in the algebra, and proving the correctness of the identities".*

Array Theory, he further claimed, though without actually using the terminology, is a theory of algebraic invariants:

> *"Array Theory explores certain intrinsic properties of data by means of identities for operations on arrays".*

In this theoretical development, he pointed out that:

> *"The central problem of Array Theory has been to define simultaneously the structure of arrays, the effect basic operations have on arrays, and the transformation of basic operations by operators so that as many facts as possible of this nature hold without exception for all arrays and all operations".*

The major result of his endeavours to solve this problem, he summed up as follows:

> *"The principal finding of array theory is that most structural facts about ordinary arrays continue to hold unchanged at the boundaries where nesting effectively terminates or where arrays become empty or singular. The intuition one has about ordinary arrays applies also to the exotic arrays at the boundary. This means that one can usually forget about what happens at or near the boundaries – considerations that are a major source of error and consume a disproportionate amount of time".*

More's emphasis on set theory in his publications on Array Theory, its relationship to APL, and the novelty of its conception, seem to have confused the issue. For example, in an excellent survey of extensions to APL, Karl Fritz Ruehr related Array Theory to the current development in these words: [89])

"Much of the work on nested arrays was consolidated and rationalized with the advent of the Array Theory of Trenchard More. Although originally inspired by thoughts of extensions to APL, Array Theory has grown to become a discipline in its own right, with a syntax somewhat different than that of APL and with a flavour more akin to that of axiomatic set theory. However, some of the results of research in Array Theory have inspired further thought about extensions to APL, and the two fields remain closely linked".

Array Theory is neither some kind of set theory nor a programming language. As I see it, Array Theory is a geometry of data, developed in the sense of Klein's Erlanger Program as a theory of algebraic invariants. Thus, as Sylvester pointed out in 1864: [89])

"As all roads lead to Rome, so I find in my own case at least that all algebraic inquiries, sooner or later, end at the Capital of modern algebra over whose shining portal is inscribed the Theory of Invariants"

In order to appreciate the potential and the perspective of More's contribution, it may perhaps be appropriate briefly to call to the attention the more important demands to be satisfied by a theory in order that it may be classified axiomatically as an algebra. Put quite plainly, we may say that they are two: First, the axioms must be consistent with each other. Secondly, the axioms must be simple, few, and fruitful

To say, in the sense of mathematical logic, that the axioms must be consistent with each other, means not only that the axioms must not contradict each other, but also, what is tantamount to this, that they must not give rise to theorems which contradict each other. To establish consistency in this broad sense, is clearly a problem far exceeding that of designing a programming language.

The path followed by More to establish a rigorous theory in this sense, adds novel perspective to the role of the computer in creative mathematical work He has accomplished what some might have conceived but none have actually done: namely, to develop an entire mathematical theory using the computer interactively as a theorem-proving tool. We might discard his theory as useless, as an abstract game with meaningless symbols, yet the fact remains that this feat alone has turned a new leaf in the history of computer applications. In view of the present efforts to integrate the computer into the curricula of our highschools or gymnasia, his approach is bound to have impact on the teaching of mathematics. Some remarks to clarify the nature of his contribution are therefore in order

The axioms or postulates on which a theory must be founded, are in principle arbitrary propositions or conditions imposed on some set of fundamental concepts. Hence, the first step in the so-called *axiomatic approach*, is to decide on the basic

concepts, concerning which the statements of the theory are to be made. Unless the work is undertaken for the sheer pleasure of creating beautiful patterns, these concepts have some preconceived, usually obvious real-life interpretations. In a mathematical sense, however, they are *undefined symbols*, specifying certain abstract objects and some basic operations or relations to which the objects submit. The word "undefined" is used here to emphasize that, within the theory, no other meaning can be ascribed to these symbols but that implied by the statements of the theory. The symbols are the "meaningless" rules and pawns of the game. This guarantees that the conclusions drawn in the theory, will be independent on any interpretation.

The design of a theory is basically an iterative process, distinguishing it from the usual textbook problem of analysis of an existing theory. Having selected the undefined symbols and specified the "best" guess of potential axioms, we start developing the theory by logical deduction of consequences. These consequences are checked against each other for consistency and against the interpretation for usefulness. If the results are dissatisfactory, we go back to the beginning and change the potential axioms or the undefined symbols (usually the operations). We then start all over again, revising that part of the theory which was influenced by the changes. Either here, or in the subsequent derivation of new consequences, new "errors" are encountered and the process repeats itself. It was this problem More desired to automate by means of the computer.

In 1971, More had used an APL terminal to prove theorems on groups, semi-groups, and lattices by investigation of the associated multiplication tables along lines similar to those described in connection with figure 26. [90]) It was quite natural, therefore, that he should attempt to carry this experience over into his work on Array Theory. In particular, if these techniques of theorem-proving were applied to the multiplication table at each stage of the design process, this would automate the entire analysis of the theory.

Hence, adopting this approach More would be able to experiment with alternative sets of potential axioms and their effect on the properties of the derived operations. Or, he could determine what new operations to introduce by first filling in the table with entries giving a desired pattern, and then afterwards finding out how to specify the corresponding elements of the carrier. In effect, the theory would be developed in accordance with the principles laid down by Klein in the Erlanger Program. Of course, the multiplication table did not have to define a group, but could be a more general algebraic structure.

An important assumption mentioned earlier, is that the Erlanger Program interprets the group concept as a set of different operations performed successively on a *single* element. This assumption is important because it implies that the array is

the only object in Array Theory, just as the set is the only object in set theory. In mathematical logic, theories satisfying this property are called *one-sorted*. This does not only agree with our geometrical conception of an array as a finite manifold, but it also has the advantage that, to quote More: *"the result of any operation may be taken as an argument for any operation."*

Now, if all the arrays were tabular arrays the property of one-sortedness would cause no problems. Still, the whole point of Array Theory is that the basic object is the nested array including the tabular array as a special case. But since no other elements than the nested array can exist in the theory, a consequence of one-sortedness is that the terminal objects of a nested array must also be nested arrays. Thus, while there is little conceptual difficulty when the terminal objects do not belong to the universe of arrays, the subtleties arising from one-sortedness appear to be against common sense. Yet, to reap the advantages of a simple algebra More followed Willard V.O. Quine, his old Harvard professor in mathematical logic, and introduced *self-containment* or the concept of continued self-nesting by infinite recursion of the terminal objects. In practice, of course, we may stop this process using a conventional if-then-else construction whenever array theory is implemented in a programming language.

Although the notion of self-containment in Array Theory may seem strange at first, it should be recalled that progress is often made by critical thinkers with imagination and daring to dispense with or even override intuition and common sense. To illustrate, when Riemann formulated his geometry he substituted the Euclidean axiom of parallels by the requirement that, through a point P not on a straight line L, no parallel lines can be drawn. From this he derived two strange theorems: That all perpendiculars to a line meet in a point; and that two straight lines will enclose an area. However, if we interpret Riemann's geometry as the geometry on the familiar sphere, these two theorems become obvious, because here the undefined concept of a straight line is interpreted as a great circle. Our problem simply was that we focused on the physical image on the stretched string between two points in Euclidean space, rather than on the fact that the straight line was the shortest distance between these two points. It is exactly the last mentioned and invariant property that characterizes a geodesic and hence a great circle on the sphere

The important point now is that More was able to apply computerized theorem-proving to establish associativity of the about 250 operations he had developed. [91]) In other words, he used the computer interactively to prove that Array Theory at least has the algebraic structure of a *semigroup*. In particular, this was done for all kinds of nested arrays including the boundary case of empty arrays. To my knowledge, no other theory has been so thoroughly tested. The importance hereof

should not be underestimated. His contribution provides a consistent mathematical foundation for the dealing with data structures in all future design of programming languages. Indeed, even if we prefer to come up with another geometry of data, More has set a standard henceforth to be met.

2.11 Up to an Ordinal Scale

Abraham Fraenkel, who was in 1922 one of the early and principal developers of what came to be known as the Zermelo-Fraenkel set theory, observed in 1953 in his book on *Abstract Set Theory* that: [92])

> *"From a psychological viewpoint, there can be no doubt that somehow the* ordered *set is the primary notion, yielding the plain notion of set or aggregate by an* act of abstraction, *as though one jumbled together the elements which originally appear in a definite succession. As a matter of fact, our senses offer the various objects or ideas in a certain spatial order or temporal succession. When we want to represent the elements of an originally non-ordered set, say the inhabitants of Washington D.C., by script or language, it cannot be done but in a definite order"*.

It is interesting to reconsider the Campbell-Stevens definition of measurement in the light of this remark. On one hand, it tells us that, in our perception, the objects or events of the definition are always ordered. Yet, on the other hand, it is brought out implicitly by the content of Fraenkel's book that it is, indeed, useful to neglect that order for the purpose of investigating some of the characteristic properties of these objects or events.

Since the objects or the events define the structure of our data arrays: the axes and their relative arrangement in space, we may interpret this remark as an insight, or a hint, to investigate those properties of the axes that pertain to the nominal scale-form prior to any undertaking of an inquiry into the particular properties related to the ordinal scale-form. Clearly, this agrees with the group-theoretical definitions of the scale-forms, whereby all properties determined on the nominal scale-form are also properties on the ordinal scale-form. Paraphrasing economic terminology, we could say that, adopting this approach, the properties are determined *up to* the ordinal scale-form.

The defining property of the nominal scale-form is that it is invariant under all transformations of the symmetric group. This does *not* imply, however, that all indices of an array can be permuted at will without changing the content or meaning of the array. In fact, the result would not only be chaos, but the entire operation would defy the meaning of invariance in connection with arrays. The point is that, apart from the ravel of the array aligning all elements in principal order, an array

defines *several* nominal scales and not just one nominal scale. We can have invariance under the symmetric group of *each* of these scales, but this is clearly less general than the situation whereby also indices on one scale permute with indices on another scale

In algebra such a combination of groups, preserving the identity of each group, is known as the *direct product* (or *sum*) of the groups. Basically, the outcome of a direct product is a new group each element of which is an *N*-tuple of elements, one from each of the defining groups. The direct product group contains all possible of such *N-tuple* combinations. In fact, it is the set-theoretical Cartesian product (or, in APL terms: the outer product) of all the groups. Since by the *order* of a group we understand its size or number of elements, the order of a direct product group will be the product of the orders of the defining groups. If the defining *N* groups are denoted *A, B, C*, etc., the direct product group is written.

$$A\times B\times C\times \ldots \text{ (}N\text{ groups)}$$

Since it is in this sense that we shall consider invariance under the different nominal scales of an array, we ought to talk about invariance under the *direct product of such-and-such symmetric groups*. This, however, is so pedantic and cumbersome that it should suffice to signal this notion simply by using the plural form: *symmetric groups*. Hence, only for a list or the ravel of an array can we talk about *a* symmetric group.

For an *N*-dimensional array, we might think that the direct product would be defined by *N* symmetric groups, one for each axis. The order of each of these groups would then be the size or number of positions on the corresponding axis However, we must not forget the recursive nature of the definition of measurement; namely that the objects or events are themselves again measured with respect to something – the preconceived theoretical notion suggested by Sir Karl Popper. For an array, this preconceived notion is interpreted as the relative arrangement of the axes, their so-called *ranking*, as we list the axes to give the shape of the array. Accordingly, underlying this ordering of the axes in the shape vector: "ρA" of the array "A", yet a nominal scale exists for the array. We can conclude, therefore, that invariance of an *N*-dimensional array must be sought under the direct product of *(N+1)* symmetric groups of the appropriate orders.

In his brilliant study "*A History of Mathematical Notations*", published 1929, Florian Cajori distinguished between two kinds of symbolic or notational forms: the *primitive*, and the *incorporative*, using the latter to denote combinations of two or more of the former. [24]) We shall find it convenient to adopt this terminology in connection with our discussion of the invariance of an array under its associated symmetric groups.

TRANSPOSITION	NOTATION	INVERSE	INVARIANT
REFLECTIVE	⍉A	A←⍉⍉A	A≡⍉(⌽⍳⍴⍴A)⍉A
PERMUTATIONAL	P⍉A	A←(⍋P)⍉P⍉A	(⍴A)[⍋P]≡⍴P⍉A
REPEATED-INDEX	I⍉A	NOT DEFINED	NOT DEFINED
LEGEND	A	NON-SCALAR ARRAY	
	P	PERMUTATION OF VECTOR ⍳⍴⍴A	
	⍋P	INVERSE OF PERMUTATION P	
	I	PERMUTATION OF K,¯1↓⍳⍴⍴A	
	K	REPEAT. INDEX K←¯1↑⍴⍴A	

Figure 28 Transposition is a primitive form

Here, it is quite evident that for arrays we must further subdivide the primitive forms into two classes: One pertaining to the void data-structure (the "cells" or positions), and another relating to the assigned data (the measurements or the contents of position). Clearly, the three operations involved in the identification or transformation of shape

SHAPE: ρA
RESHAPE: DρA
RAVEL: ,A

discussed in connection with figure 21, are primitive forms belonging to the first-mentioned class.

A fourth primitive form in this class is

TRANSPOSITION: ⍉A L⍉A

which, as shown in figure 28, may be defined in three different ways. All three are denoted by the same APL symbol which intends to convey the image of a conventional transposition about the principal diagonal of a matrix

Applied in its monadic form with only a right argument, we shall call it a *reflective* transposition for obvious geometrical reasons. Originally, it submitted to a different definition. [25]) The basic problem facing the designers of APL after having introduced the notation for this monadic form, was to generalize its use from 2-dimensional matrices to *N*-dimensional arrays. In the original version, the IBM APL\360 of 1968, the monadic form yielded the array with the last two axes interchanged. In all later versions, however, the monadic transpose was taken to mean a reversal of the order of all axes of the array argument. Clearly, both interpretations were valid extensions of the conventional matrix transposition illustrated in figure 29. Why is it then that the last-mentioned form was intuitively preferred? Possibly it was for aesthetic reasons which, if true, may be explained by the symmetry underlying the corresponding invariant given in figure 28. Incidentally, this invariant in terms of a reversal, is found too in the so-called many-valued logic

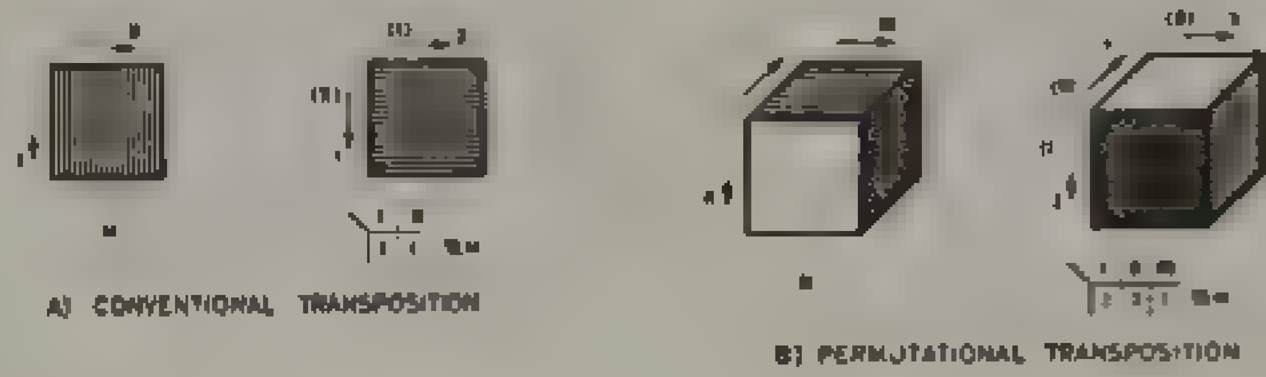


Figure 29. Reflective and permutational transposition

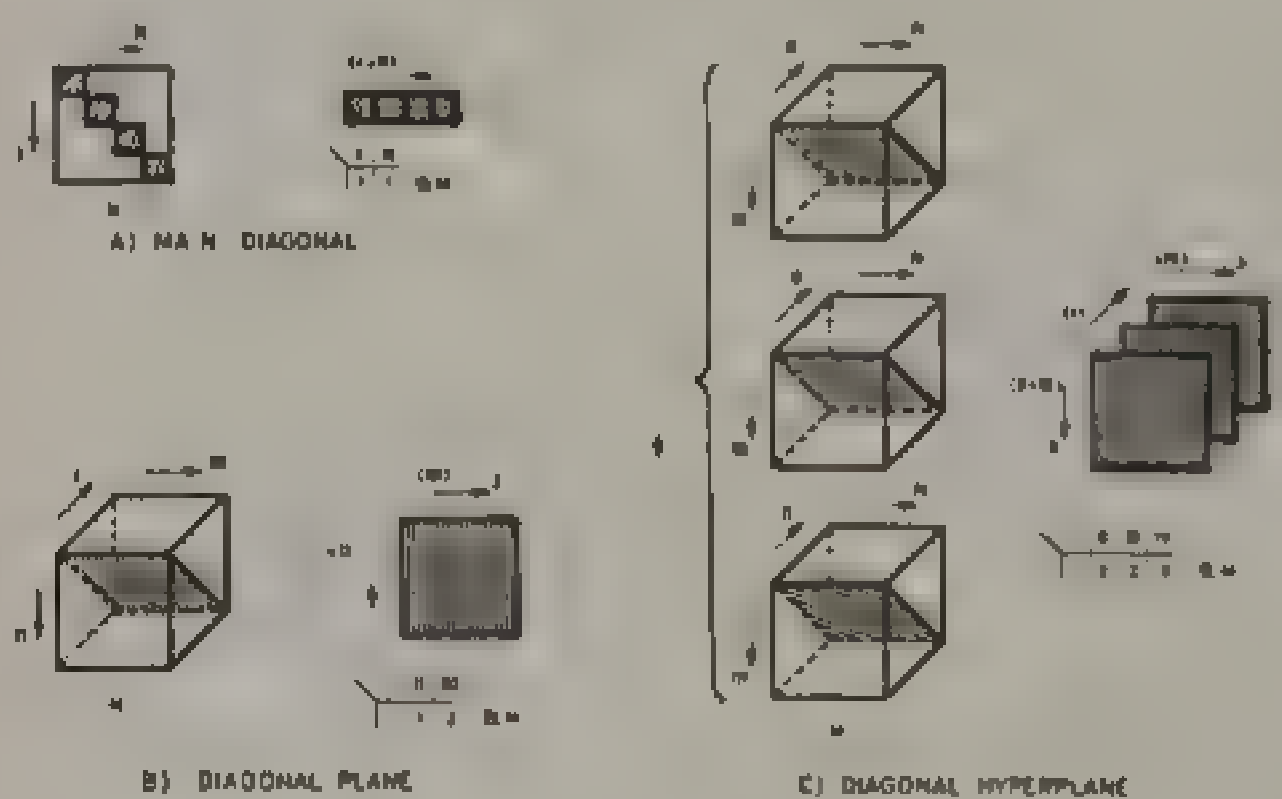


Figure 30. Repeated-index transposition on matching axes

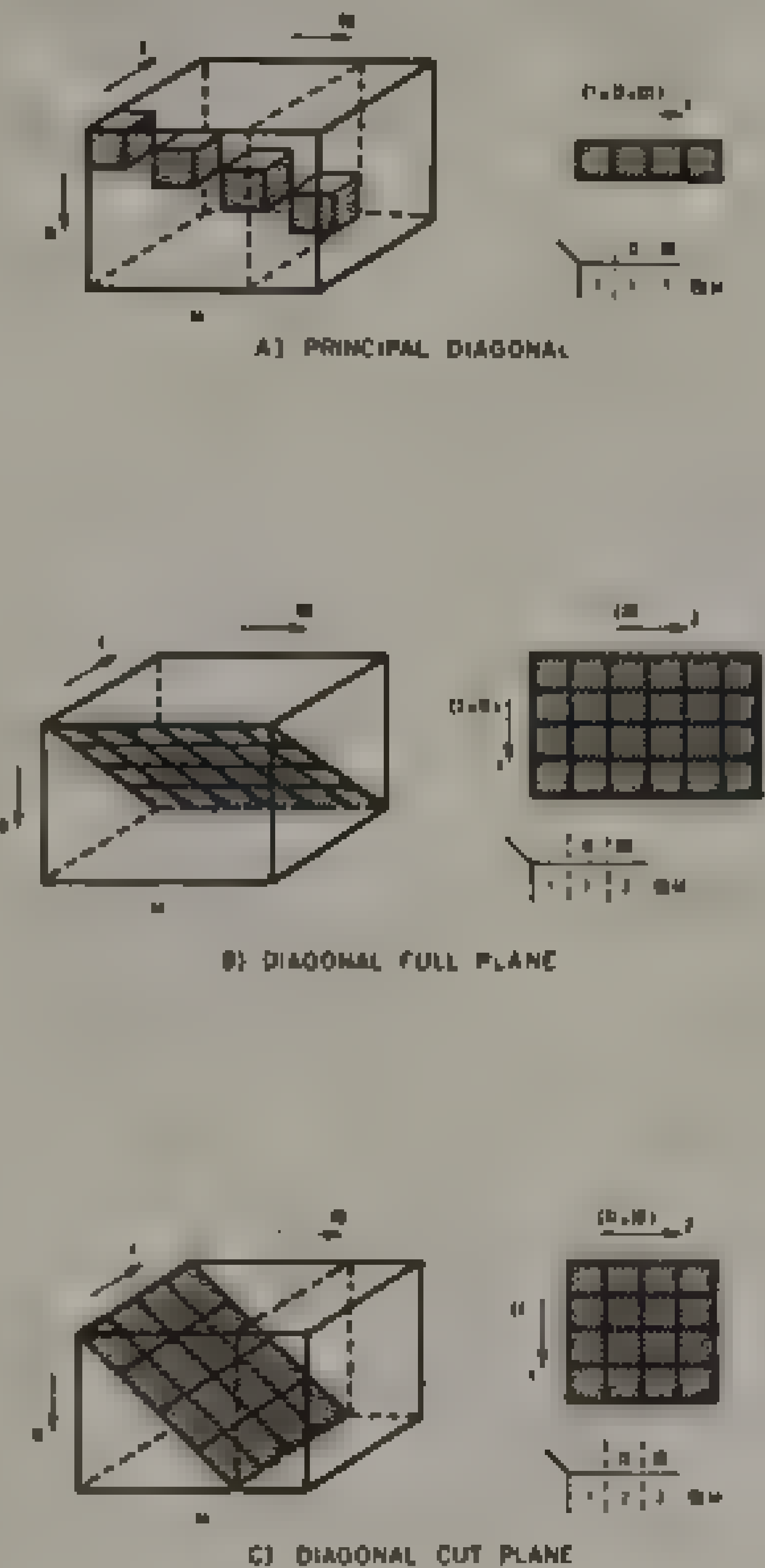


Figure 31. Repeated-index transposition on non-matching axes.

```
THE PRIMITIVE ARRAY GENERALIZATIONS OF THE
SCALAR BINARY PRODUCT   + × ∨ ∧ ⌈ ⌊  THAT
ARE INVARIANT UNDER THE SYMMETRIC GROUP,
ARE THE OUTER PRODUCT AND THE REDUCTION

                SCALAR PRODUCT
                     X□Y
                     / \
                    /   \
                   /     \
        OUTER PRODUCT     REDUCTION
           X∘.□Y           □/X,Y

FOUR REDUCTIONS ARE STANDARD MATHEMATICAL
EXPRESSIONS

 CARTESIAN VECTORS     BOOLEAN QUANTIFIERS
   SUM       +/V        EXISTENTIAL   ∨/P
   PRODUCT   ×/V        UNIVERSAL     ∧/P
```

Figure 32 Array operations on primitive forms.

where it is interpreted as a generalization of the famous *law of the double denial* from Boolean algebra. But more about that later.

The *permutational* transposition which is also exemplified in figure 29, represents a more general extension of conventional matrix transposition. In fact, as explained in the figure, it includes the monadic form as a special case. The specification in figure 28 of the invariant of this form, demonstrates that although it implements the fundamental substitution formula of the theory of permutations, it happens to do it such that the axes are permuted by the *inverse* permutation of P rather than, as in the algebra, by P itself. For a matrix, of course, this is unimportant because the permutation 2 1 is its own inverse. [94])

Whereas these two forms of transposition are invariant under the symmetric group of the ranking order of the array, this does not apply to the *repeated index* transposition which only submits to the more general structure of a monoid or a semigroup. Still, in spite of the loss of information by this kind of transposition, it is perhaps the most important of them all. In particular, this operation is a cornerstone of the powerful index notation of tensor algebra, brought to perfection by Einstein and others. As demonstrated in figures 30 and 31, this transposition applies in APL and elsewhere for the repeated index, specifying axes that match, or do not match, in size

The problems of defining primitive forms for operations on the contents of the "cells" in a data-array, is basically a matter of generalizing the well known binary operation for scalars, so that it becomes invariant under the appropriate permutations. Since the latter may apply either for all axes or only for a single axis, this gives rise to the two primitive forms shown in figure 32. The *outer product* is evidently the invariant under the "all-axes" permutations, since it pairs each member of its left argument with each member of its right argument. Alternatively, the *reduction* is invariant under the "single-axis" permutations, since basically it is the "sum" or "product" of all elements along the axis.

It is thought-provoking in this connection that the *outer product* was introduced into APL only by a lucky incident, in spite of the fact that in tensor algebra it is the fundamental operation, implementing the Cartesian product of Cantor's set theory. Thus, changing Iverson's original APL notation to that of today, we may quote him for the following statement on his original position in 1962 after he had abolished the distinction between row and column vectors in APL [61]):

> *"The question whether a vector enters a given operation as a row vector or as a column vector is normally settled by the requirement of conformability, and no special indication is required ... The question remains, however, in the case of the two vector operands, which may be considered with the pre-operand either as a row (as in the scalar product Y+.×X) or as a column. The latter case produces a matrix Z and will be denoted by*
>
> $Z \leftarrow Y \circ . \square X$
>
> [adding in a footnote that since] *no scan operator is required, the symbol ∘ may be interpreted as the 'null' scan".*

The most frequent and versatile incorporative forms are the *contraction*, the *addition*, and the *inner product*. Their relationships are explained in figure 33. The contraction is only recognized in APL as a composite function, having no distinct symbol assigned to it. Yet, in tensor algebra it is considered as fundamental as the outer product. Thus, according to the mathematical physicists J. L. Synge and A. Schild: [95]) *"The inner product is obtained from the outer product by the process of contraction"*. However, as demonstrated in the figure, it is more convenient and general to select reduction as a primitive form rather than contraction. Of course, this is only possible because APL has extended the conventional transposition to repeated-index transposition.

Addition is another incorporative form. It may be convenient to introduce it in the teaching in terms of the conventional "element-to-element" explanation. However, unless countermanded at a later stage of the education, this bars the way to further insight in APL as a mathematical notation. For example, it is the conception of addition as an incorporative form, that explains the addition of a vector to the rows or columns of a matrix by a mathematical argument which in turn can be generalized. [96]) Of course, we may be forced to implement it the "programming way", but having understood it as a distinct mathematical concept, we can now deal

```
IMPORTANT INCORPORATIVE FORMS IN APL. ARE THE
INNER PRODUCT, THE ADDITION, AND A TENSORIAL
OPERATION KNOWN AS CONTRACTION  DERIVED FROM
THE PRIMITIVE FORMS OF REDUCTION, REPEATED
INDEX TRANSPOSITION, AND OUTER PRODUCT, THEY
ARE RELATED BY SOME KIND OF  ASSOCIATIVE LAW
ON THE PRIMITIVE FORMS IN THE SAID ORDER

CONSIDER THE TWO SCALAR OPERATIONS  ◊  AND  ⎕
(SUCH AS  + × ∨ ∧ ⌈ ⌊) ON THE TWO NON SCALAR
ARRAYS  A  AND  B  WITH
   N=×/(ρA),ρB   &   I=1 2   ,K,K,, ,(N 1)
WHERE DIMENSION  K  IS  OR IS NOT, A MATCHING
DIMENSION OF  A  AND  B

               REPEATED INDEX
REDUCTION      TRANSPOSITION       OUTER PRODUCT
  ◊/[K] ,           I⍉ ,,          A∘.⎕B
                    |
                    |
            \       |       /
MATCHING       INNER PRODUCT          NON MATCHING
INDEX K     A◊.⎕B↔◊/[K]I⍉A∘.⎕B         INDEX K

                  /   \

      CONTRACTION          ADDITION
        ◊/[K]I⍉            ◊/[K]I⍉A∘.⎕B

THUS, ONLY THE STANDARD NOTATION FOR ADDITION
AND INNER PRODUCT REQUIRES A MATCHING INDEX K

ADDITION HAS SOME REMARKABLE INTERPRETATION
IN BOOLEAN ALGEBRA  FOR EXAMPLE, CONSIDER THE
DEFINITION OF DISJUNCTION, THE  OR  OPERATION
IN TERMS OF IMPLICATION   (P≤Q)≤Q.  IN APL
INTRODUCING THE TRUTH TABLE FOR IMPLICATION BY
THE OUTER PRODUCT   L∘.≤L  WITH  L←0 1.  WE
MAY WRITE THIS DEFINITION   1 2 2⍉(L∘.≤L)∘.≤L
ASSIGNING PROPOSITION P INDEX 1 AND Q INDEX 2

ANOTHER INTERESTING INCORPORATIVE FORM IS THE
SO-CALLED DIRECT MATRIX PRODUCT WHICH COMBINES
THE PRIMITIVE FORMS OF RESHAPE,  PERMUTATIONAL
TRANSPOSITION, AND OUTER PRODUCT   THUS, IF  A
AND  B  ARE TWO MATRICES WE HAVE IN  1 ORIGIN

          DIRECT MATRIX PRODUCT
         ((ρA)×ρB)ρ1 3 2 4⍉A∘.⎕B

CLEARLY, THIS FORM IS INVARIANT UNDER A  GROUP
RATHER THAN UNDER A MONOID OR SEMIGROUP AS THE
INCORPORATIVE FORMS LISTED ABOVE
```

Figure 33. Array operations on incorporative forms.

with it as a unit in our thinking. Also, we often find that mathematicians have been doing a lot of the thinking for us, so that time and again not only do we reinvent the wheel but we do not even notice it. For instance, the addition of two matrices in terms of scalar multiplication, is known in the mathematical literature as the *Schur product* after the German mathematician. [97]) This form of addition has important applications in crystallography.

The inner product has been discussed earlier, so let us go directly to the last incorporative form on figure 33, namely the so-called *direct matrix product*. Basically, this product provides a matrix representation of the direct product of group theory that we introduced previously. For APL users who need a real number representation of a complex number matrix algebra, the direct matrix product provides an elegant tool of transformation. [13]) However, what is of interest here, is that it could not work in this application except for the fact that it is invariant under a group. It is this property which guarantees a one-to-one correspondence between the two representations.

A conspicuous characteristic of the invariant forms discussed here, is that none of them deals explicitly with the array coordinates or indices. Their purpose is to handle the array as a unity: an entire geometrical figure in space; and if we are concerned with only part of an array, they describe that part by geometrical considerations of symmetry. In fact, the question of coordinates becomes explicit only when we focus on the individual points of an array. This is the obvious way to deal with all physical things in the world around us. It is also the natural way to treat data collections. Nevertheless, it will be instructive to see what a coordinate representation of one of these forms looks like.

The basic invariant in APL was the dimensional identity of an array under shape transformations, that we discussed in connection with figure 21. In his book published in 1962, Iverson suggested an elegant coordinate representation of this form, based on a generalization of the mathematical notion of a positional number system. [61]) That is, the indices of an N-tuple of coordinates are conceived as the "digits of a number" which, transformed into the decimal system, gives the position in the ravel of the array. Iverson's solution to this problem is given in figure 34.

Positional number systems are discussed in detail in any mathematics textbook on the highschool or gymnasium level, so it will suffice here to highlight a couple of important points. One obvious complication is that the base value (which is ten for the decimal system) changes from position to position. In fact, for a given position it is the size of the corresponding axis of the array. If we consider the possible different "digits" that may occur on a given position, it is likewise evident that they must belong to the sequence of positive integers from zero to one less the base value (thus, in the decimal system, the ten figures from zero to nine). As it may

```
POINT IDENTIFICATION IN 0 ORIGIN BETWEEN AN
N TUPLE (I,J,K,...) OF A NON EMPTY ARRAY  A
AND A SCALAR INDEX  P  OF ITS RAVEL  ,A

            A[I,J,K,...] = (,A)[P]

AND PRINCIPAL ORDER ARE PRESERVED UNDER THE
INVERSE TRANSFORMATIONS

     DECODE             P = (ρA)⊥I,J,K...
     ENCODE  (I,J,K,...) = (ρA)⊤P

ALSO CALLED BASE VALUE AND REPRESENTATION
RESPECTIVELY.

TO ILLUSTRATE, CONSIDER THE EXAMPLE
      ⎕IO←0
      A                    ,A
 4 1 0               4 1 0 7 3 8
                           ρ,A
 7 3 8               6
      ρA
2 1 3

HERE, THE SEQUENCES OF N-TUPLES  (I,J,K)
AND CORRESPONDING SCALAR INDICES  P,  ARE
      N←  ρA  ι×/ρA        N←   ⊤ ρA ρ(,A ιT
 0 0 0               0
 0 0 1               1
 0 0 2               2
 1 0 0               3
 1 0 1               4
 1 0 2               5

WHICH SHOULD BE COMPARED ROWWISE, SAY
      (ρA)⊤5               (ρA)⊥1 0 2
 1 0 2               5
      A[1,0,2]             A[5]
8                    8

MATHEMATICALLY, THIS APPROACH GENERALIZES
THE POSITIONAL CONCEPT OF NUMBER SYSTEMS
SUCH AS THE DECIMAL, BUT IT FAILS FOR EMPTY
ARRAYS. THAT IS, ONLY THE  NON-EMPTY  SPACE
OR SUB ARRAY TO THE RIGHT OF THE RIGHT MOST
0 IN THE SHAPE VECTOR, IS PRESERVED IN THE
INVERSE TRANSFORMATIONS

A BASIC CAUSE FOR THIS, IS THAT THE ENCODE
FUNCTION IS FOUNDED ON THE RESIDUE FUNCTION
AND  HENCE, INVOKES THE SPECIAL DEFINITION
OF APL   N|0↔N  FOR AN EMPTY AXIS
```

Figure 94. APL index transformations.

be seen in the mathematics textbooks, this sequence is actually the principal remainders after division by the base value. In his book, Iverson discussed this transformation quite thoroughly, and he introduced the function, now called *decode* in APL, to implement it. Simultaneously, he remarked that "*since the process is based on a positional representation of the key* [read: *N*-tuple], *it will be convenient to use 0-origin indexing for all operands*". The inverse transformation, the *encode* function, was not conceived at the time he wrote the book

Two things are important to note at this point. First, the transformation is based on the residue concept of division. Secondly, this makes it convenient to adopt a 0-origin indexing instead of the 1-origin that we have used hitherto.

Perhaps the reader will recall at this point that, both in the discussion of the book cipher and in the quotation by Vandermonde on his choice of integer assignments for his indices, it was natural to assign the number "1" to the first element along an axis. From the use of APL, the reader is undoubtedly familiar with the use of both origins, so that it does not bother him whether the first element is assigned the index "0" or "1". After all, an index is merely a label selected from the sequence of natural numbers. For Vandermonde and his contemporaries, however, such an assignment was utterly nonsense. To them zero had the physical implication of "nothing". It was therefore inconceivable that the first element, which undoubtedly existed, could be thus assigned. May we imagine that Babbage was thinking along these lines when his work on the Difference Engine led him into algebraic considerations of what in retrospect we interpret as a generalization of the residue concept from 0- to 1-origin. I think so.

Babbage published his results late 1822 in two letters to the editor in *Brewster's Journal of Science* and in the *Memoirs of the Astronomical Society*,[86] respectively. Thus, he wrote Dr. Brewster:

> *"I had mentioned to you that, before I left London, I had completed a small engine which calculated tables by means of differences. On considering this machine, a new arrangement occurred to me, by which an engine might be constructed that should calculate tables of other species, whose analytical laws were unknown. On this suggestion, I proceeded to write down a table which might have been made, had such an engine existed; and finding that there were no known methods of expressing its nth term, I thought the analytical difficulty which was thus brought to light, was itself worthy of examination"*

Babbage's new arrangement which he humorously described as the engine "*eating its own tail*", was later implemented mechanically. As we see his invention today, it was the first "programming" facility for recursive computation. [65] One of the series which Babbage envisaged that his revised engine could handle, he described as follows:

"... it is the equation

$$\Delta u_z = \textit{units fig. } u_z$$

whose integral is

$$u_z = 20b + 2^a$$

where a is that one of the numbers 1, 2, 3, 4, which, taken from z, leaves the remainder divisible by 4, and b is the quotient of that division".

whereupon he gave the first 9 terms of the series.

Figure 35 simulates the execution of this prescription in APL. It is evident from this figure as well as from his quotation, that he was actually introducing a transformation of the principal remainders to a 1-origin.

What is important here, is that Babbage did not see this as an isolated result. On the contrary, he related it to his topological inquiries and, particularly significant, he referred it to the array of "cells" described by Vandermonde

> *"Amongst the singular and difficult equations of finite differences to which these series led, I recognised one which I had several years since met with, in an analytical attempt to solve a problem considered by Euler and Vandermonde; it relates to the knight's move at chess. At that time, I had advanced several steps; but the equation in question proved an obstacle I was then unable to surmount. In its present shape, although I have not yet deduced the solution from the equation, yet, as I am in possession of the former, it is not too much to anticipate a general process applicable to this class of equations; and should that be the case, I shall be able to advance some steps further in a very curious and difficult inquiry, connected with the geometry of situation".*

Even more striking, perhaps, is Babbage's concluding note, transmitting his vision of the importance of his invention across the ocean of time:

> *"Thus, you see, one of the first effects of machinery adapted to numbers has been to lead us to surmount new difficulties in analysis; and should it be carried to perfection, some of the most abstract parts of mathematical science will be called into practical utility, to facilitate the formation of tables. The more I examine this theoretical part, the more I feel convinced that it will be long before the novel relations which it presents will be exhausted; and if the absence of all encouragement to proceed with the mechanism I have contrived, shall prove that I have anticipated too far the period at which it shall become necessary, I will yet venture to predict that a time will arrive when the accumulating labour which arises from the arithmetical applications of mathematical formulæ, acting as a constant retarding force, shall ultimately impede the useful progress of the science, unless this or some equivalent method is devised for relieving it from the overwhelming incumbrance of numerical detail."*

Even if this simple example was all that Babbage ever published on his generalization of the residue concept under division, it was not a chance observation, a


```
IN 1822 BABBAGE CONSIDERED A FIRST ORDER
DIFFERENCE EQUATION
          U[Z+1]←U[Z]+ΔU[Z]
OF A NOVEL KIND
        ΔU[Z]←UNITS FIGURE OF U[Z]


THUS, ASSUMING THE FIRST TERM
                  U[1]←2
HE CALCULATED THE SERIES

       Z  |  1  2  3  4  5  6  7  8  9
          +
     U[Z] |  2  4  8 16 22 24 28 36 42
    ΔU[Z] |  2  4  8  6  2  4  8  6  2


HE ALSO EXPRESSED THE GENERAL TERM IN AN
ANALYTICAL FORM
             U[Z]←(20×B)+2*A
RELATING THE TWO CONSTANTS TO  Z  BY
                 Z = A+B×4
SUCH THAT DIVISION OF  Z  BY THE NUMBER
 4 , YIELDS THE QUOTIENT  B  AND THE
PRINCIPAL REMAINDER   A = 1,2 3, OR 4


IN APL, ASSUMING 1-ORIGIN
      ⎕IO←1

WE FIND FOR THE INDEX SEQUENCE
      ⎕←Z←⍳9
1 2 3 4 5 6 7 8 9

AND THE CORRESPONDING REMAINDERS
      ⎕←A←1+4|Z-1
1 2 3 4 1 2 3 4 1

THAT THE QUOTIENTS ARE
      ⎕←B←(Z-A)÷4
0 0 0 0 1 1 1 1 2

ALTERNATIVELY, THEREFORE, THE SERIES MAY
BE CALCULATED
      ⎕←U←(20×B)+2*A
2 4 8 16 22 24 28 36 42

WITH ITS FIRST ORDER DIFFERENCES
        1↓U    ¯1↓U
2 4 8 6 2 4 8 6
```

Figure 35. Babbage's generalization of the residue concept.

lucky stroke, the deeper significance of which escaped him. Babbage's writings on his computers, the Difference Engine and the Analytical Engine, bristle with numerical illustrations; and, as a closer study will reveal, he put his soul into them to explain his ideas. Whether published or merely in manuscript form, Babbage's examples form the key to a deeper understanding of his scientific contribution: from mathematics, over his computers, and to ciphers.

At the inauguration of a new university faculty at Lille on December 7th, 1854, Louis Pasteur said with explicit reference to the discovery of electromagnetism by Hans Christian Ørsted, that "*In the field of observation, chance favours none but the prepared mind*". [98] This remark fits Babbage too. His contribution to the residue concept derives from a very deep and thorough study of the underlying theory of congruences. But even more significant, this study was the fountainhead sustaining his endeavours to create a mathematical model of substitution ciphers.

The notion of congruence appears in the works of Euler, Lagrange, and Legendre. But it was Gauss who introduced its notation; systematized its theory and extended it; classified the problems to which it applied; and demonstrated how to use it in attacking these problems. This we find in his publication of 1801, his monumental *Disquisitiones arithmeticae*, the book that created the modern theory of numbers. Gauss was only twenty-four when this masterpiece, some say his greatest, appeared in print. Quite incredibly, however, he finished most of the manuscript at the age of twenty. The story goes that he submitted it to the French Academy who rejected it. Nevertheless, a thorough search in 1935 of the permanent records of the Academy disproved this story once and for all. The work was never submitted, much less rejected. This finding also agrees with Lagrange's enthusiasm when on May 31st, 1804, he wrote Gauss,

> "*Your* Disquisitiones *have raised you at once to the rank of the first mathematicians, and I regard the last section as containing the most beautiful analytical discovery that has been made for a long time ... Believe me, Sir, that no one applauds your success more sincerely than I*".

For mortals of a lesser standing than Lagrange, Gauss' work is hard to comprehend. In fact, it is generally agreed by mathematicians that the *Disquisitiones* make very difficult reading. It is therefore fortunate that Gauss' friend and successor in the chair at Göttingen, the mathematician Peter Gustav Lejeune Dirichlet, spent so much time and effort on expounding it. Since Gauss' work itself has been called a "*book of seven seals*", Dirichlet is recognized today as the first who broke the seals. Though, when Babbage as a young and hopeful mathematician undertook his study of Gauss' book, this was still in the future. To see Babbage in this perspective, is to appreciate his accomplishment.

According to Tucker's catalogue, Babbage's library contained seven mathematical books by Gauss. Six of these are the original editions in Latin of different works, published in the period 1799 to 1832. Among them we find the *Disquisitiones* from 1801. A French translation of the latter by A.C.M. Poullet-Delisle, constitutes the seventh book, published in Paris in 1807 under the title: *Rescherches arithmétiques*.

Commenting on this translation in the catalogue, Tucker writes: "*A celebrated and now very scarce work ... Some MSS solutions in the volume*". This remark is noteworthy, because Babbage's books rarely contained autographic material. So perhaps we may infer that the translation was Babbage's working copy, purchased quite early in his life. By the same token, the Latin editions were probably acquired at a much later time, when Babbage had more or less given up his mathematical studies. For example, Gauss' doctoral thesis and very first publication from 1799 is marked "*uncut*" by Tucker. One edition from 1818, and two from 1828, described in terms such as "*in loose sheet*" or "*paper wrapper*" in the catalogue, might even have been presented to Babbage by Gauss personally during their sojourn in Berlin in 1828.

Among 400 other participants, both attended in that summer a German-Scandinavian conference on science, organized by the famous explorer and pioneer of international scientific cooperation, Alexander von Humboldt. The still existing list of signatures of the participants has Gauss on its first page next to Hans Christian Ørsted who on previous occasions had been visiting with him in Göttingen. [99] During a visit in London in 1823, Ørsted had been closely associated with Babbage through the latter's intimate friend, John Herschel. Chances are, therefore, that Ørsted was instrumental in bringing Gauss and Babbage together.

Babbage's early study of Gauss' notion of congruence of numbers, placed him among the first mathematicians to take a serious interest in this important aspect of number theory. Undoubtedly, he saw in this topic, at least intuitively, fundamental ideas that might aid him in the mechanical design of his computers.

The notion of congruence of numbers is basically an algebraic counterpart of our conception of "sameness" of geometrical figures or, as it is called technically, *congruence* (Latin: to coincide or agree). In all its simplicity, the algebraic idea is that two integers "*a*" and "*b*" are the "same", or congruent, if divided by a third integer "*m*" they both leave the same remainder. In other words, the difference of the two integers, "$a - b$", is divisible by the third integer "*m*". It follows that the common divisor "*m*" is a kind of "unit" for measuring the sameness of "*a*" and "*b*". To emphasize this relationship, Gauss introduced the term: *modulus* (Latin, small measure), abbreviating it *mod*, to denote the common divisor "*m*". Thus, instead of writing the relationship of congruence,

$$a = b + q \times m$$

he left out the integral quotient "q" as algebraically insignificant, in that he introduced the standard notation of today:

$$a = b \ (mod\ m)$$

This expression is read: "*a is congruent to b modulo m*". If it satisfies the very special condition that "a" is less than "m", but simultaneously greater than or equal to zero, then "b" represents the so-called *principal remainder* upon division of "a" by "m". Very often, however, merely the term: *remainder* is used. Figure 36 provides a more precise description of these notions.

Gauss was not only among the greatest of all mathematicians. He was also a very practical man, inspired to some of his most sublime deeds by his dealing with physical or engineering problems. Thus, for a period of five years, from 1821 to 1825, he was entrusted by King George IV of Hannover and England to survey the German realm, penetrating himself, in all kinds of weather, woods and other terrain with no main roads at all. Gauss not only succeeded, but to cope with the necessities of the job, he conjured up new ideas in measurement techniques and geometry. In a similar vein, his work on congruence of numbers stems from real-life considerations.

The clock-face of a watch, or the odometer giving the mileage of a car, are everyday devices illustrating the idea. Their usefulness derives from the fact that instead of counting from zero to eternity, they begin all over again every time they have reached 12 (24) hours or 99,999 kilometers, respectively. Thus, it may be amusing but not very practical to inform you that I put these lines in print some time after 17,381,640 o'clock, telling the time of the day by counting the hours since that special event in Bethlehem some two thousand years ago. Less cumbersome is it to say that it is shortly after midnight on such-and-such a day

That is, considering an infinite sequence of integral hours we put them into a finite number of classes, each characterized by a distinct remainder; namely, the number giving the time of the day. From this point of view, we cannot distinguish between different members in a given class. They are all the "same" in the sense that they represent 4 o'clock p.m., say. Hence, congruence is an equivalence relation. It establishes a measure of the time of the day on a nominal scale. If in addition these classes are ordered relatively by som further rule, establishing a scale of precedence among them, the measurement of the time of the day is performed up to an ordinal scale

The usually neglected fact that *two* rules are involved, is of paramount importance. The notion of congruence provides no more than the equivalence relation defining a nominal scale-form. This is a distinct property, entirely different from the relative ordering superimposed upon the equivalence classes by some second rule. It is the introduction of this second rule which brings the measurement of


```
ALGEBRAIC CONGRUENCE PARTITIONS NUMBERS INTO EQUIVALENCE
CLASSES, DESIGNATED THE  RESIDUE CLASSES , THE NUMBER OF
CLASSES IS MEASURED BY AN INTEGER, SAY M, KNOWN AS THE
 MODULUS . THE RESIDUE CONCEPT PROVIDES A NOMINAL SCALE
REPRESENTATION OF THE CLASSES, ASSIGNING EACH CLASS A
TYPICAL OF ITS MEMBERS, SAY R, THE SO-CALLED  PRINCIPAL
REMAINDER

HENCE, GIVEN A MODULUS  M,  AN ARBITRARY NUMBER  X  IS
ASSIGNED A PRINCIPAL REMAINDER  R,  SATISFYING THE RULE
                              X=R+Q×M
WHERE  Q  IS AN INTEGRAL QUOTIENT. BY WAY OF TERMINOLOGY
THIS IS EXPRESSED BY SAYING THAT  R  IS THE 'RESIDUE OF
X  MODULO  M , WRITING
    R=X (MOD M)     OR, EQUIVALENTLY IN APL.     R←M|X

SINCE ALL REMAINDERS IN A CLASS ARE CONGRUENT OR SIMILAR
WHEN MEASURED BY THE MODULUS,  THE CHOICE OF A PRINCIPAL
REMAINDER  R  TO REPRESENT THE CLASS, IS TRADITIONALLY
DETERMINED BY THE REQUIREMENT
    0≤R<M      OR, EQUIVALENTLY IN APL:      (0≤R)∧R<M

EVIDENTLY, THIS MAKES THE RESIDUE FUNCTION   M|X, ORIGIN
INDEPENDENT.  THUS, FOR MODULUS   M=4  CONSIDER THE FOUR
RESIDUE CLASSES  OF NUMBERS  X  IN EITHER ORIGIN
      X
   8   4   0   4   8  12
   7   3   1   5   9  13
   6  ¯2   2   6  10  14
   5   1   3   7  11  15

      ⎕IO←0                                ⎕IO←1
      4|X                                  4|X
0 0 0 0 0 0                          0 0 0 0 0 0
1 1 1 1 1 1                          1 1 1 1 1 1
2 2 2 2 2 2                          2 2 2 2 2 2
3 3 3 3 3 3                          3 3 3 3 3 3

THAT IS, THE THIRD COLUMN OF X IS SELECTED AS A NOMINAL
SCALE.  THE PRINCIPAL REMAINDERS,  TO PROVIDE A MEASURE
OR REPRESENTATION OF THE FOUR CLASSES
      X[;2]                                X[;3]
0 1 2 3                              0 1 2 3

THE ALGEBRAIC EXTENSION TO CONGRUENCE OF FRACTIONS, MAY
BE ILLUSTRATED IN APL
      4|7.45             4|¯7.45           1|7.45
3.45              0.55               0.45
THE LATTER, INCIDENTALLY, IS A CONVENIENT WAY OF FINDING
THE NON-INTEGRAL PART OF A POSITIVE NUMBER.

SPECIAL APL DEFINITIONS ARE THE EXTENSIONS TO A ZERO OR
A NEGATIVE MODULUS
      0|4               ¯4|3              ¯4|¯7.45
4                 ¯1                ¯3.45
```

Figure 36. The algebraic notion of congruence.

A MORE FLEXIBLE CHOICE OF NOMINAL SCALE REPRESENTATION IS THE SO-CALLED "J-RESIDUE MODULO M", DEFINED BY

```
    J≤R<J+M    OR, ALTERNATIVELY IN APL    (J≤R)∧R<J+M
```

WHERE J IS AN ARBITRARY INTEGER

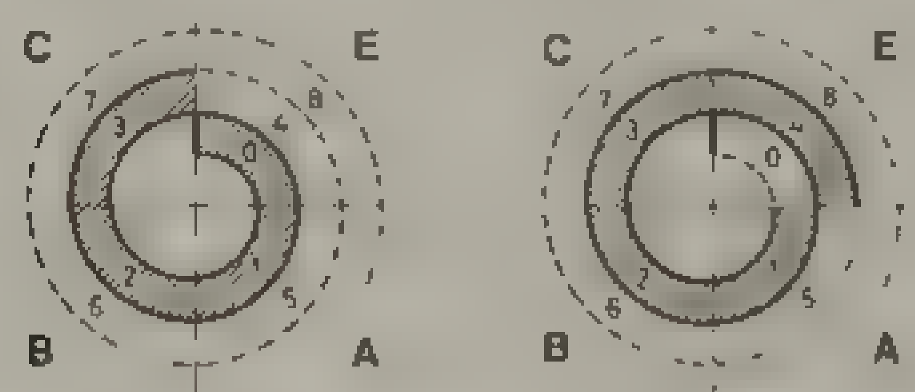
A FUNCTION IMPLEMENTING THE J-RESIDUE, MAY BE DEFINED AS FOLLOWS, WITH A NUMERICAL, 2-ELEMENT VECTOR JM←J,M AS LEFT ARGUMENT, THE ARRAY OF NUMBERS X AS RIGHT ARGUMENT, AND THE J-RESIDUES MODULO M AS THE RESULT R

```
                ∇ RESIDUE[⎕] ∇
              ∇ R←JM RESIDUE X;⎕IO;J;M
        [1]  ORIGIN ⎕IO←0
        [2]  ARG J←1↑JM
        [3]   M←1↓JM
        [4]  REST R←((-J)⌽J+⍳M)[(M)|X]
              ∇
```

THE BASIC PURPOSE OF THE J-RESIDUE IS TO INTRODUCE THE ORIGIN DEPENDENT INDEX GENERATOR ⍳M, AS THE NOMINAL SCALE REPRESENTATION OF THE PRINCIPAL REMAINDERS. THUS, FOR CONGRUENCE OF NUMBERS X MODULO M=4, CONSIDER THE FOUR EQUIVALENCE CLASSES LABELLED EABC, RESPECTIVELY

```
      L← EABC
      L ,X
E  ¯8  ¯4   0   4   8  12
A  ¯7  ¯3   1   5   9  13
B  ¯6  ¯2   2   6  10  14
C  ¯5  ¯1   3   7  11  15

      ⎕IO←0                           ⎕IO←1
      L,⍉(⎕IO,4) RESIDUE X            L,⍉(⎕IO,4) RESIDUE X
E 0 0 0 0 0 0                   E 4 4 4 4 4 4
A 1 1 1 1 1 1                   A 1 1 1 1 1 1
B 2 2 2 2 2 2                   B 2 2 2 2 2 2
C 3 3 3 3 3 3                   C 3 3 3 3 3 3
```

GEOMETRICALLY, THESE FOUR CLASSES MAY BE VISUALIZED AS THE QUADRANTS OF A SPIRAL, SHAPED BY THE NUMBERS X



A) 0 RESIDUE   B) 1 RESIDUE

Figure 37 The j-residue modulo m.

SINCE THE INDEX ASSIGNMENT OF AN ALPHABET L SATISFIES THE IDENTITY ⍳⍴L←→L⍳L IN EITHER ORIGIN, AN ALPHABET IS A CONVENIENT WAY OF REPRESENTING AN ORDINAL SCALE.

ASSUME THAT THE J-RESIDUE CLASSES OF CONGRUENCE MODULO (⍴L) SUBMIT TO AN ORDINAL SCALE REPRESENTED BY, SAY, THE FOUR-LETTER ALPHABET L←'EABC'. THAT IS, 4=⍴L. THEN, UNDER CHANGE OF ORIGIN, THE SCALE TRANSFORMATIONS WHICH KEEP THE SCALE-FORM INVARIANT, ARE CYCLIC SHIFTS

THUS, STIPULATING THE INDEX ASSIGNMENT

```
      0-ORIGIN  0 1 2 3            1 ORIGIN  1 2 3 4
                ↓ ↓ ↓ ↓                      ↓ ↓ ↓ ↓
                E A B C                      E A B C
```

WE SEE THAT INTERPRETATION OF THE INDEX VECTOR ⍳⍴L AS THE SEQUENCE OF PRINCIPAL REMAINDERS IN EITHER ORIGIN, ACTUALLY IMPLIES THAT, TO PRESERVE THE SCALE-FORM, THE TWO ORDINAL SCALE REPRESENTATIONS MUST BE

```
         RESIDUE CLASSES      | 0-ORIGIN | 1-ORIGIN
         ---- -----------     +--        +    -
      0   4  (8  12  16 . )  |    E     |    C
      1  (5   9  13  17   )       A     |    E
      2  (6  10  14  18 . )  |    B     |    A
      3  (7  11  15  19   )       C     |    B
```

IT FOLLOWS THAT, WHEREAS ALPHABET L DOES INDEED DENOTE THE ORDINAL SCALE OF THE PRINCIPAL REMAINDERS IN THE 0-ORIGIN, IT DOES NOT DO SO IN THE 1-ORIGIN.

HENCE, WORKING IN 1-ORIGIN, WE MUST CYCLICALLY SHIFT THE ALPHABET L ONE POSITION TO THE RIGHT IN ORDER TO USE IT AS A SCALE FOR THE PRINCIPAL REMAINDERS. THUS,

```
      ⎕IO←1
      L                                ⍳4
EABC                               1 2 3 4
        ¯1⌽L                             ¯1⌽⍳4
CEAB                               4 1 2 3
                                         L[¯1⌽⍳4]
                                   CEAB
```

ALTERNATIVELY WE MAY USE THAT CONGRUENCE MODULO (⍴L) IS AN EQUIVALENCE RELATION COMPATIBLE WITH ADDITION THAT IS, WE CAN INTRODUCE "ADDITION MODULO (⍴L)" AS A BINARY OPERATION ON THE PRINCIPAL REMAINDERS

```
      (⎕IO,⍴L) RESIDUE ¯1+⍳4           (⍴L)| 1+⍳4
4 1 2 3                            0 1 2 3
      L[(⎕IO,⍴L) RESIDUE ¯1+⍳4]          ⎕←A←4×0=(⍴L)|¯1+⍳4
CEAB                               4 0 0 0
                                         L[A+(⍴L)| 1+⍳4,]
                                   CEAB
```

Figure 38. Invariance under change of origin

congruence up to the ordinal scale-form characteristic of the clock-face or the odometer. However, the second rule is brought in so naturally, so inconspicuously, that we hardly notice it. We merely count, from zero and upwards, the hours of the day, or the distance traversed in kilometers by a car. Both are causal measures of the irreversibility of time, that everything grows older, that there is an order which cannot be reversed. We take it for granted but, strictly speaking, this order is additional to the nominal scale measurement we have established in terms of residue classes.

Since the principal remainders representing the residue classes, are the integers from zero to one less the modulus, it is almost second nature to consider them the ordered sequence of integers produced by APL's index generator: "ι*M*" in a 0-origin. Still, it might be just as desirable, or perhaps even mandatory, like in the days of Vandermonde and later of Babbage, to represent the residue classes by the sequence of integers from *one* to the modulus included. That is, to identify their representation with the outcome of the index generator: "ι*M*" in a 1-origin. Babbage's example simulated in figure 35, is probably the earliest instance in the mathematical literature of such a transformation of the residue concept. Independently, Iverson took up the idea in 1962 and generalized it under the name of a *j-residue*. Thus, he wrote: [61])

> *"In classical treatments ... only the 0-residue is considered. The use of 1-origin indexing accounts for the interest of the 1-residue"*

Figure 37 explains the pertinent details of this generalization. From the definition of a *j*-residue it is evident that, basically, the entire notion is independent of any consideration of the index origin. This is as it should be for a nominal scale representation. However, what is of interest to us, is the quite arbitrary relationship that may be introduced by interpreting the index sequence "ι*M*" in a *j*-origin as the *j*-residue principal remainders.

Of course, in practice "*j*" can merely be zero or one. Since zero is the standard textbook case, all that really matters, is what happens in 1-origin. The geometrical illustration shown in the figure, provides a simple explanation. If we imagine that the sequence of integers are mapped onto a spiral, the latter can then be divided into radial sections so that each section contains all integers in the same equivalence class. As shown by the hatched areas in the figure, it is now a simple matter to select the origin-dependent set of principal remainders. In particular, the choice to the left in A) is Gauss' classical residue, whereas the option to the right in B) is Babbage's generalization. To be able to speak about the equivalence classes independently of the choice of origin, it is convenient to label them by the letter of an alphabet.


```
SINCE CONGRUENCE TO A MODULUS IS AN EQUIVALENCE RELATION
COMPATIBLE WITH THE BINARY OPERATIONS OF ADDITION AND
MULTIPLICATION,  THE STUDY OF LINEAR EQUATIONS MAY BE
EXTENDED TO CONGRUENCES

OF PARTICULAR INTEREST IN CONNECTION WITH SUBSTITUTION
CIPHERS, IS THE ESTABLISHMENT OF A MULTIPLICATION TABLE
FOR  ADDITION OF CONGRUENCES .  WITH THE CARRIER DEFINED
BY AN ALPHABET, SAY   L←'EABC'  WITH  4=⍴L,  THE PROBLEM
IS TO LET THE ALPHABETIC INDEX VECTOR   ι⍴L  OR  LιL,
REPRESENT THE PRINCIPAL REMAINDERS, YET, SIMULTANEOUSLY,
KEEP THE ALPHABETIC REPRESENTATION OF THE MULTIPLICATION
THE SAME IN EITHER ORIGIN.

      L←'EABC'                ¯1⌽L                   1⌽L
                      CEAB                   ABCE

                         TABLE OF ADDITION

      ⎕IO←0                   ⎕IO←1
      M ← ι⍴L)∘. +ι⍴L         M1←( ⍴L)∘. +ι⍴L
      (⍴L)|M0                 (⎕IO,⍴L) RESIDUE M1
0 1 2 3               2 3 4 1
1 2 3 0               3 4 1 2
2 3 0 1               4 1 2 3
3 0 1 2               1 2 3 4
      D←T←L[(⍴L)|M0]          ∧/,T=(¯1⌽L)[(⎕IO,⍴L) RESIDUE M1]
EABC                  1
ABCE                          (⎕IO,⍴L)RESIDUE ¯1+M1
BCEA                  1 2 3 4
CEAB                  2 3 4 1
                      3 4 1 2
                      4 1 2 3
                              ∧/,T=L[(⎕IO,⍴L) RESIDUE ¯1+M1]
                      1

                        TABLE OF SUBTRACTION

      N0←(ι⍴L)∘.- ι⍴L         N1←(ι⍴L)∘.- ι⍴L
      (⍴L)|N0                 (⎕IO,⍴L) RESIDUE N1
0 3 2 1               4 3 2 1
1 0 3 2               1 4 3 2
2 1 0 3               2 1 4 3
3 2 1 0               3 2 1 4
      D←S←L[(⍴L)|N0]          ∧/,S=(1⌽L)[(⎕IO,⍴L) RESIDUE N1]
ECBA                  1
AECB                          (⎕IO,⍴L) RESIDUE 1+N1
BAEC                  1 4 3 2
CBAE                  2 1 4 3
                      3 2 1 4
                      4 3 2 1
                              ∧/,S=L[(⎕IO,⍴L) RESIDUE 1+N1]
                      1

 OBSERVE FOR THE TWO MULTIPLICATION TABLES THAT   S= 1⌽⍉T
```

Figure 39. Addition and subtraction of congruent integers.

The consequences hereof are explained in figure 38. The surprising conclusion is that the alphabet represents the ordinal scale in a 0-origin, but that it fails to do so in a 1-origin. Here we have to rotate the alphabet cyclically to preserve the ordinal scale-form. This leads to further complications.

A standard topic in any highschool or gymnasium textbook on mathematics, is that an equivalence relation is *compatible* with a binary operation. The meaning of this expression is that the result of combining two equivalence classes by a binary operation does not depend on the choice of representation. To be sure, two principal remainders can be added (or multiplied) by simply forming their sum (or product) in the ordinary sense, if only afterwards we "reduce" the result to the appropriate remainder. Indeed, barring certain restrictions concerning the existence of an inverse under multiplication, we can establish an entire algebra of remainders.

However, the complications propagate as soon as we leave the refuge of the textbook presentation and begin to explore the consequences in a 1-origin. Figure 39 demonstrates two alternative ways of coping with these problems. One approach is to *subtract 1* under addition, or *add 1* under subtraction. The other, which more explicitly reveals what is actually happening, is merely to cyclically *rotate* the alphabet *clockwise* under addition, and *anti-clockwise* under subtraction. The purpose of the residue function in this connection, is simply to substitute the principal remainder of value zero by that of the modulus itself. Evidently, this can also be done by brute-force programming, like it is done at the bottom of figure 38.

The transformation to a 1-origin is instructive, because it brings out the implicit assumptions of invariance of scale-form. Yet, in actual practice it is clumsy and inconvenient, and must be discarded in favour of working in a 0-origin.

There is, however, a far deeper significance to the 1-origin approach demonstrated here. The fact is that what I have presented in these few figures, is a mathematical description summarizing Babbage's approach such as I have been able to deduce it from his manuscript computations. Thus, after having simulated all his details in APL, filling out the gaps and identifying the significant special cases, I can assure the reader that Babbage preferred to use the technique of adding or subtraction a 1, but that he, at least in one instance, also rotated the alphabet. Similarly, he consistently used the brute-force method of substituting zero by the modulus as principal remainder, usually in the last step of his computations. None of his many manuscripts which I have examined, carries the slightest trace of a 0-origin indexing. It appears safe to conclude, therefore, that the idea never occurred to him. On the contrary, whatever notes he left, they are all concerned with the transfer of the residue concept to a 1-origin.


```
THE DEFINING PROPERTY OF THE ORDINAL SCALE-FORM, IS THAT
IT IS INVARIANT UNDER THE  MONOTONIC GROUP .  THIS TERM
IS NOT STANDARD IN THE MATHEMATICAL LITERATURE  IN THAT
IT IS BUT A POPULAR DESCRIPTION COMBINING TWO FAMILIES OF
RELATED GROUPS,  KNOWN AS  CYCLIC  AND  DIHEDRAL  GROUPS
RESPECTIVELY, OF COURSE, SINCE WE ARE CONSIDERING ONE OR
MORE AXES OF AN ARRAY, WE USUALLY HAVE A DIRECT PRODUCT
OF SUCH GROUPS

THE ESSENCE OF THESE GROUPS, IS THAT THEY ARE GENERATED
BY ONLY TWO PRIMITIVE OPERATIONS  REVERSAL AND ROTATION,
BOTH OF WHICH ARE ORDER PRESERVING. THUS, ROTATION IS THE
COMMON GENERATOR OF BOTH KINDS OF GROUPS, WHEREAS THE
REVERSAL OR  FLIP  OPERATION IS THE ADDITIONAL GENERATOR
TAKING US FROM CYCLIC GROUPS TO DIHEDRAL (MEANING  TWO
SIDES )

MANY-VALUED LOGIC PROVIDES THE INITIAL INTERPRETATION OF
ORDINAL SCALE INVARIANCE, NAMELY OF TRUTH VALUES, UNDER
THESE TWO GENERALIZATIONS OF BOOLEAN NEGATION

                        BOOLEAN NEGATION
                              ~L
                         (1 0  ↔ 0 1)
                       /              \
            0         /                \       0
MIRROR-IMAGE   | ↑   /                  \     / \   POSTIAN
OR INVERSION   ↓ |  ⌽L                  ¯1⌽L  \ /   OR CYCLIC
  NEGATION     1     \                  /      1    NEGATION
                    LAW OF DOUBLE DENIAL
                          L = ~~L

IN GENERAL, SUBSTITUTING THE TRUTH-VALUE REPRESENTATION
OF THE ORDINAL SCALE BY AN  ALPHABET , SAY  L, THE  LAW
OF DOUBLE DENIAL   BECOMES THE THREE DEFINING RELATIONS

               ALPHABET OR ORDINAL SCALE   L
                          GENERATORS
                        /            \
          REVERSAL   ⌽L              ROTATION   ¯1⌽L
            (FLIP)                    (CYCLIC SHIFT)

                   DEFINING RELATIONS BY
                    LAW OF DOUBLE DENIAL
                      /              \
               L = ⌽⌽L   (1)            L = (-⍴L)⌽L   (2)
                       \
                     L = ¯1⌽⌽¯1⌽⌽L   (3)

A SIMPLE EXAMPLE ILLUSTRATING THE LATTER RELATIONSHIP IS
FURNISHED BY THE GROUP TABLE OF THE AUTOMOBILE EXAMPLE,
HERE, IT REPRESENTS THE VECTOR L OF INVERSE STRATEGIES

           L                ¯1⌽⌽L               L
     EABC             ECBA               ECBA
```

Figure 40. Reversal and rotation are primitive forms.

Our discussion of invariance under the ordinal scale-form would not be complete, unless we characterized the defining group (or family of groups) and established the primitive forms of the associated operations. This is done in figure 40 which demonstrates that there are two primitive forms under this scale in APL:

ROTATION: $N\phi L$

REVERSAL: ϕL

The latter, in fact, was discussed previously in connection with the definition of transposition.

Perhaps the most fascinating aspect of these two primitive forms, is that they appear explicitly in this basic role in the mathematical theory of many-valued logic. In this discipline, since they act as negations, they are derived by generalization of the negation in Boolean algebra. Here, the fundamental invariance is the *law of double denial*. It testifies to the consistency of the notion of scale-form invariance, that this law expands into the defining relations of the associated groups. [100] We shall later find occasion to come back to these groups from a more convenient viewpoint, actually bringing them to use. Hence, we shall postpone the discussion until then

In his *Scientific Autobiography* from 1946, Max Planck remarked that a new scientific truth is not accepted because the opponents become convinced and declare themselves educated, but rather because they die out, and the rising generation is brought up with the fact. [101] To this we should perhaps add that a scientific contribution can be evaluated only in a perspective. The greater the man, the greater the perspective. Babbage's vision certainly has influenced our way of life. Hence, to provide a gauge for his work, has been the aim of our excursion into the geometrical nature of data.

2.12 APL Terminal Session

Mathematically, there is but a small step from Bishop Wilkin's discussion of transposition ciphers to Babbage's interest in the topological properties of magic squares and the knight's tour. Exploring this connection in APL, we proceed with a related example, namely the grille invented by Cardano. Though we use the grille to produce a cryptogram rather than to conceal the message in the wordings of an inconspicuous text. Julius Petersen's fractionating cipher provides ample opportunity for illustrating Cantor's diagonal process of ordering as well as APL's encode and decode functions. Finally, we demonstrate how very simply the group axioms may be tested by text editing and subsequent application of APL's execute function.


```
        ⍝        * * * ROUTE TRANSPOSITIONS * * *

        ⍝ THE TRANSPOSITION CIPHERS DESCRIBED BY BISHOP WILKINS
        ⍝ IN 1641 ARE BASICALLY ALL ROUTE TRANSPOSITION CIPHERS

        ⍝ RECONSIDERING HIS EXAMPLES IN APL, WE SHALL ALSO FIND
        ⍝ OCCASION TO DEAL WITH THE KNIGHT S TOUR AND THE MAGIC
        ⍝ SQUARE DISCUSSED BY BABBAGE

        ⍝ ALTERNATING LINES

        ⍝ TO PRODUCE ALTERNATING ROWS OR COLUMNS, WE INTRODUCE
        ⍝ A MATRIX OF ALTERNATING ROWS AS A BASIS FOR FURTHER
        ⍝ GEOMETRICAL TRANSFORMATIONS. THUS,
        CCALTERNATE
A TRANSPOSITION INDEX MATRIX  M  WITH ALTERNATING
ROWS OF DIMENSION  DIM  IS PRODUCED

        ∇ ALTERNATE[⎕] ∇
      ∇ M←ALTERNATE DIM
[1]     M←((⌈ 1↑DIM÷ 2) ⍴  1↑DIM)⍴⍳× DIM
[2]     M←DIM⍴(0 ¯1 0 ↓M),[⎕IO+1]⊖ 0 1 0 ↓M
      ∇

        ⍝ TO ACCOMMODATE WILKINS' FIRST EXAMPLE WE PROCEED AS
        ⍝ FOLLOWS
        ⍴⎕←M←ALTERNATE 10 10
   1   2   3   4   5   6   7   8   9  10
  20  19  18  17  16  15  14  13  12  11
  21  22  23  24  25  26  27  28  29  30
  40  39  38  37  36  35  34  33  32  31
  41  42  43  44  45  46  47  48  49  50
  60  59  58  57  56  55  54  53  52  51
  61  62  63  64  65  66  67  68  69  70
  80  79  78  77  76  75  74  73  72  71
  81  82  83  84  85  86  87  88  89  90
 100  99  98  97  96  95  94  93  92  91
10 10
        ⍴⎕←⊖⍉M
 100  81  80  61  60  41  40  21  20   1
  99  82  79  62  59  42  39  22  19   2
  98  83  78  63  58  43  38  23  18   3
  97  84  77  64  57  44  37  24  17   4
  96  85  76  65  56  45  36  25  16   5
  95  86  75  66  55  46  35  26  15   6
  94  87  74  67  54  47  34  27  14   7
  93  88  73  68  53  48  33  28  13   8
  92  89  72  69  52  49  32  29  12   9
  91  90  71  70  51  50  31  30  11  10
10 10

        ⍝ THE MESSAGE WAS
        ⍴⎕←TW KNS]
THE PESTILENC DOTH STILL INCREASE AMONGST VS.
WEE SHALL NOT BE ABLE TO HOLD OUT THE SIEGE
WITHOUT FRESH AND SPEEDY SUPPLIE.
3 45
```

```
      ⍝ WHERE IN PASSING WE NOTE THAT, ALTHOUGH THE EDITOR
      ⍝ OF THE 1802 EDITION REVISED BISHOP WILKINS' ARCHAIC
      ⍝ SPELLING, HE DID NOT TOUCH THE ENCIPHERED MESSAGES

      ⍝  CLEANING  THE MESSAGE
      ⍴LW←PUNCTUATION TWLKNS1
9 .35
      ⍴TC←LW REMOVE TWLKNS1
100

      ⍝ WE FIND IN AGREEMENT WITH WILKINS
      ⍴⎕←TC[⍉⍳M]
ERFDLEFLLT
IETOOSWITH
LSUDHSNTE
PHTLAVLSP
PAPT LTRHE
UNTHE SETS
SDIELNGADT
YSWSHONSLI
EPEIATOECL
FEGEEBMANE
10 10

      ⍝ RAIL FENCE CIPHER

      ⍝ WILKINS' NEXT ILLUSTRATION IS MERELY A MATTER OF
      ⍝ RESHAPING THE  CLEANED' TEXT INTO A 2 COLUMN MATRIX
      ⍝ WHICH IS THEN TRANSPOSED. THUS,
      ⍴⎕←TWLKNS2
THE SOULDIERS ARE ALLMOST FAMISHED,
SUPPLY VS, OR WEE MUST YIELD
2 35
      ⍴LW←PUNCTUATION TWLKNS2
9 70
      ⍴TC←LW REMOVE TWLKNS2
52
      ⍴⎕←⍉26 2⍴TC
TEOLIRAELMSFMSESPLVOWEUTIL
HSLDESRALOTAIHDLPYSREMSYED
2 26

      ⍝ THE NAME  RAIL FENCE CIPHER  WHICH WAS INTRODUCED
      ⍝ DURING THE AMERICAN CIVIL WAR, DERIVES FROM THE
      ⍝ ZIGZAG ROUTE FORMED BY THE PLAINTEXT
      2 40↑⍉((3×⍴TC)+2),2)⍴((3×⍴TC)⍴1 0 0)\TC
T E O L I R A E L M S F M S
 H S U D E S R A L O T A I

      ⍝ CORNER CIPHER

      ⍝ WILKINS' LAST EXAMPLE IS BASED ON A ROUTE TRAVERSING
      ⍝ THE CORNERS OF A  DIMINISHING  RECTANGLE
```



```
      PRINT WLKNS3
1  9 17 25 33 41 49 57 65 67 59 51 43 35 27 19 11 3
5 13 21 29 37 45 53 61 69 71 63 55 47 39 31 23 15 7
6 14 22 30 38 46 54 62 70 72 64 56 48 40 32 24 16 8
2 10 18 26 34 42 50 58 66 68 60 52 44 36 28 20 12 4
      ⍴WLKNS3
4 18

      ⍝ THUS, FOR THE MESSAGE
      ⍴⎕←TWLKNS3
WEE SHALL MAKE AN IRRUPTION VPON THE ENIMIE FROM
THE NORTH, AT TEN OF THE CLOCK THIS NIGHT.
2 48
      ⍴LW←PUNCTUATION TWLKNS3
9 96
      ⍴TC←LW REMOVE TWLKNS3
72

      ⍝ WE FIND
      ⍴⎕←TC[WLKNS3]
WMRPITAHHSCTEINPKE
HAIHFONOIHKFTOENIL
ANOERROEGTTTHMNVRL
EALOMHTEINLENETTES
4 18

      ⍝ KNIGHT'S TOUR

      ⍝ THE EXAMPLE PROVIDED BY BABBAGE IS
      ⍴⎕←KNIGHTSTOUR
 42 57 44  9 40 21 46  7
 55 10 41 58 45  8 39 20
 12 43 56 61 22 59  6 47
 63 54 11 30 25 28 19 38
 32 13 62 27 60 23 48  5
 53 64 31 24 29 26 37 18
 14 33  2 51 16 35  4 49
  1 52 15 34  3 50 17 36
8 8

      ⍝ THUS, IF THE MESSAGE IS THE FIRST 64 LETTERS OF
      ⍝ WILKINS' LAST EXAMPLE
      2 32⍴M←64↑TC
WEESHALLMAKEANIRRUPTIONVPONTHEEN
IMIEFROMTHENORTHATTENOFTHECLOCKT
```

```
⍝        * * * ROUTE TRANSPOSITIONS * * *

      ⍝ THE CRYPTOGRAM IS
      ρ⎕←M[KNIGHTSTOUR]
HHNMMIRL
FATEDLOT
EETOOCAT
KOKEPTPR
NACNUNHH
NTEVHOFU
NIETRISA
WEIMETRE
8 8

      ⍝ MAGIC SQUARE

      ⍝ HERE WE INTRODUCE A FUNCTION THAT MAY BE EXPLAINED
      ⎕[MAGICSQUARE
A MAGIC SQUARE  R  OF ODD ORDER  N  IS PRODUCED
THE  MAGIC  PROPERTY IS THAT, WHEN ADDED BY ROWS
COLUMNS, OR PRINCIPAL DIAGONALS, I E.
    +/R,   +⌿R,   +/1 1⍉R   AND   +/1 1⍉⌽R
THE SUM IS ALWAYS  N×(1+N*2)÷2

      ⍝ THE FUNCTION IS DEFINED
      ∇ MAGICSQUARE[⎕] ∇
    ∇ R←MAGICSQUARE N ⎕IO
[1]  ASSUME ⎕IO←1
[2]  EVEN →(0=2|N)/0
[3]  ODD R←(⍳N)-⌈N÷2
[4]   R←R⌽R⌽⍳N N)ρ⍳N*2
    ∇

      ⍝ NOTICING THAT THE MAGIC SQUARE FROM THE FRIGATE
      ⍝  LOSSEN , WRECKED IN 1717, WAS
      ρ⎕←⊖MAGICSQUARE 3
 6 1 8
 7 5 3
 2 9 4
3 3
      ⍝ WE PROCEED HERE TO ONE OF ORDER 7
      ρ⎕←MAGICSQUARE 7
 30 39 48  1 10 19 28
 38 47  7  9 18 27 29
 46  6  8 17 26 35 37
  5 14 16 25 34 36 45
 13 15 24 33 42 44  4
 21 23 32 41 43  3 12
 22 31 40 49  2 11 20
7 7

      ⍝ LET THE MESSAGE NOW BE THE FIRST 49 LETTERS OF
      ⍝ WILKINS' LAST ILLUSTRATION
      ρ⎕←M←49↑C
WEESHALLMAKEANIRRUPTIONVPONTHEENIMIEFROMTHENORTHA
49
```



```
⍝        * * * A TURNING GRILLE * * *

      ⍝ AND IT WILL BE ENCIPHERED
      ρ⎕←M[MAGICSQUARE 7]
EOHWAPT
RTLMUHH
RALROIF
HNRPMEO
AIVIHNS
INNTEFE
OLMAEKT
7 7

      ⍝ IT MAY AMUSE THE READER TO INVESTIGATE HOW THIS
      ⍝ CRYPTOGRAM, AND THOSE ABOVE, ARE DECIPHERED BY
      ⍝ USING THE INVERSE PERMUTATIONS


      ⍝        * * * A TURNING GRILLE * * *

      ⍝ A GRILLE MAY BE REPRESENTED BY A BOOLEAN MATRIX,
      ⍝ DESIGNATING HOLES BY 1'S AND NO-HOLES BY 0'S
      ρ⎕←G
 0 1 0 0
 0 0 1 0
 0 0 0 1
 1 0 0 0
4 4
      ⍝ TO ILLUSTRATE ITS USE, LET THE MESSAGE BE
      ρM←'TURNINGTHEGRILLE'
[illegible]
      ⍝ THEN, WRITING IN FOUR LETTERS FOR EACH CLOCKWISE
      ⍝ TURN OF THE GRILLE, WE PROCEED AS FOLLOWS
      (ρG)ρ(,G)\M[⍳4]
 T
  U
   ■
■
      (ρG)ρ(,⊖⍉G)\M[4+⍳4]
I
   N
  G
 T
      (ρG)ρ(,⊖⊖G)\M[8+⍳4]
   H
E
 G
  R
      (ρG)ρ(,⍉⊖G)\M[12+⍳4]
  I
 L
L
   E
```

```
      ⍝          * * * THE PETERSEN CIPHER * * *

      ⍝ THUS, IN EFFECT WE HAVE FOLLOWED THE ROUTE
      ⍴⎕←R←(⍴G)⍴⍋⍋,G+(2×⌽⍉G)+(3×⊖⌽G)+4×⊖⍉G
  5  1 13  9
 10 14  2  6
 15 11  7  3
  4  8 12 16
4 4
      ⍝ FILLING IN THE MESSAGE
      M[R]
ITIH
ELUN
LOGR
NTRE
      ⍝ WHICH TAKEN OFF ROWWISE YIELDS
      ,M[R],' '
ITIH ELUN LOGR NTRE


      ⍝          * * * THE PETERSEN CIPHER * * *

      ⍝ TO ILLUSTRATE JULIUS PETERSEN S FRACTIONATING CIPHER
      ⍝ WE SHALL ADOPT THE EXAMPLE FROM HIS PUBLICATION IN 1875

      ⍝ HENCE, ASSUMING WITH PETERSEN THAT WE HAVE A 1 ORIGIN
      ⎕IO←1
      ⍝ WE SHALL INTRODUCE A 25 LETTER ALPHABET (DROPPING  W )
      ⍴⎕←ABC
[illegible]

      ⍝ HIS KEY WORD OR KEY SENTENCE
      ⍴⎕←KEY
[illegible]
14
      ⍝ AND HIS PLAINTEXT MESSAGE
       [illegible]
LE PROBLEME DE DETERMINER COMBIEN IL Y A DE NOMBRES
PREMIERS COMPRIS ENTRE DEUX NOMBRES DONNES N EST PAS
ENCORE RESOLU QQ
\
      ⍝ WITH THE LATTER EXTENDED, AS PRESCIBED BY HIM, BY THE
      ⍝ DOUBLED DUMMY LETTER  Q .

      ⍝ PETERSEN S GRADE UP FUNCTION

      ⍝ A SIMPLE FUNCTION IMPLEMENTING HIS GRADE UP, IS THIS
      ∇ GRADE[⎕] ∇
    ∇ IKEY←ABC GRADE KEY  [illegible]
[1]  ORIGIN ⎕IO←1
[2]   IKEY←⍋⍋ABC⍳⌽KEY
    ∇
```

```
      ⍝          * * * THE PETERSEN CIPHER * * *

      ⍝ THUS, APPLYING IT TO HIS KEY, WE FIND
      ⍴⎕←ABC GRADE KEY
7 3 5 9 14 10 2 12 6 1 8 13 4 11
14
      ⍝ WHICH SHOWS THAT, IN A STRICT APL SENSE, IT IS REALLY
      ⍝ A REVISION OF THE EXPRESSION
      ⍴⎕←⍋⍋ABC⍳KEY
6 2 5 9 13 10 3 11 7 1 8 14 4 12
14

      ⍝ THE CHECKERBOARD ALPHABET

      ⍝ THE PURPOSE OF A CHECKERBOARD IS TO PROVIDE A 2-DIGIT
      ⍝ REPRESENTATION OF A RANDOMIZED ALPHABET.

      ⍝ A CONVENIENT FUNCTION, INTRODUCING PETERSEN S APPROACH,
      ⍝ MAY BE THIS
      ∇ CHECKERBOARD[⎕] ∇
    ∇ IABC←ABC  CHECKERBOARD KEY ROW,COL
[1]   KEY←[illegible] KEY
[2]   ROW←ABC GRADE⌽ 5↑KEY
[3]   COL←ABC GRADE 5↑KEY
[4]   IABC←,(10×ROW)∘.+COL
    ∇
      ⍝ THE RESULT OF THIS FUNCTION, IS A REPRESENTATION OF THE
      ⍝ RANDOMIZED ALPHABET AS A LIST OF CHECKERBOARD COORDINATE
      ⍝ PAIRS

      ⍝ TO SEE THIS, WE SHALL GO INSIDE THE FUNCTION DURING ITS
      ⍝ EXECUTION. THUS, TO PREPARE FOR THIS, SET
      S∆CHECKERBOARD←4

      ⍝ WE THEN INVOKE THE FUNCTION
      IABC←ABC CHECKERBOARD KEY

CHECKERBOARD[4]
      ⍝ NOW, WE HAVE IN EFFECT FOUND THE KEYS FOR RANDOMIZING
      ⍝ THE CHECKERBOARD
      [illegible]
5 2 1 4 3
      [illegible]
3 1 4 5 2
      ⍝ WHICH ARE APPLIED IN PRINCIPLE
      (5 5⍴ABC)[⍋ROW;⍋COL]
LOKMN
GUFHI
VZLXY
QTPRS
BEACD

      ⍝ HENCE, CLEANING UP THE STOP CONTROL
      S∆CHECKERBOARD←⍳0
      ⍝ WE CONTINUE THE EXECUTION OF THE FUNCTION
      →⎕LC
```

```
⍝          * * * THE PETERSEN CIPHER * * *

      ⍝ WHICH PROVIDES US WITH THE INDEX REPRESENTATION
      ⍴⎕←IABC
53 51 54 55 52 23 21 24 25 22 13 11 14 15 12 43 41 44
      45 42 33 31 34 35 32
25

      ⍝ THE ENCIPHERMENT PROCESS

      ⍝ WHEREAS THE CHECKERBOARD ALPHABET IS ESTABLISHED, SO
      ⍝ TO BREAK,  ONCE FOR ALL , THE ENCIPHERMENT BASED ON
      ⍝ THIS CHECKERBOARD IS REPEATED FOR EACH MESSAGE AS
      ⍝ FOLLOWS

      ⍝ TO BEGIN WITH IT IS ASSUMED THAT, AFTER HAVING BEEN
      ⍝  CLEANED  FOR SPACES AND SYMBOLS, THE MESSAGE IS
      ⍝ RESHAPED INTO A SQUARE MATRIX EXTENDED BY DUMMIES OR
      ⍝ NULLS AS NECESSARY
      ⍴⎕←TXT
LEPROBLEM
DEDETERMIN
ERLOMBIENI
LYADENOMBR
ESPREMIERS
COMPRISENT
REDEIXNCNB
RESDONNESN
ESTPASENCO
RERESOLUOU
10 10

      ⍝ FRACTIONATING THE COORDINATE PAIRS

      ⍝ USING THE CHECKERBOARD ALPHABET WE FIRST PERFORM
      ⍝ A SIMPLE SUBSTITUTION
      ⍴⎕←ITXT←IABC[ABC⍳,TXT]
11 52 43 44 12 51 11 52 14 52 55 52 55 52 42 52 44 14
      25 15 52 44 54 12 14 51 25 52 15 25 11 35 53 55
      52 15 12 14 51 44 52 45 43 44 52 14 25 52 44 45
      54 12 14 43 44 25 45 52 15 42 44 52 55 52 33 34
      15 12 14 51 44 52 45 55 12 15 15 52 45 15 52 45
      42 43 53 45 52 15 54 12 44 52 44 52 45 13 11 33
      41 41
100

      ⍝ THIS IS FOLLOWED BY A FRACTIONATING OF THIS LIST
      ⍝ INTO A CORRESPONDING LIST OF 1-DIGIT NUMBERS
```



```
⍝          * * * THE PETERSEN CIPHER * * *

      ⍴⎕←ITXT← 0 10 10⊤ITXT
1 1 5 2 4 3 4 4 1 2 5 1 1 1 5 3 1 4 5 2 5 5 5 2 5 5
      5 2 4 2 5 2 4 4 1 4 2 5 1 5 5 2 4 4 5 4 1 2 1
      4 5 1 2 5 5 2 1 5 2 5 1 1 3 5 5 3 5 5 5 2 1 5
      1 2 1 4 5 1 4 4 5 3 4 5 4 3 4 4 5 2 1 4 2 5 5
      2 4 4 4 5 5 4 1 2 1 4 4 3 4 4 2 5 4 5 5 2 1 1
      4 2 4 4 5 2 5 5 5 2 3 3 3 4 1 5 1 2 1 4 5 1 4
      4 5 2 4 5 5 5 1 2 1 5 1 5 5 2 4 5 1 5 5 2 4 5
      4 2 4 3 5 3 4 5 5 2 1 5 5 4 1 2 4 4 5 2 4 4 5
      2 4 5 1 2 1 1 3 3 4 1 4 1
200

      ⍝ DIAGONAL ROUTE TRANSPOSITION

      ⍝ TO DEFINE THE DIAGONAL ROUTE, LET US INTRODUCE
      ⎕ DIAGONAL
A DIAGONAL TRANSPOSITION INDEX MATRIX  M  OF DIMENSION  DIM
IS PRODUCED. BEGINNING IN THE UPPER LEFT CORNER, THE ROUTE
PROCEEDS BY UPWARD DIAGONALS FROM LEFT TO RIGHT. SEVEN OTHER
DIAGONAL PATTERNS MAY BE PRODUCED SUBSTITUTING EITHER OR
BOTH GRADE DOWNS    ⍒   BY GRADE UP    ⍋   OR/AND '+  BY
THE INVERSE OF THIS MATRIX   M   IS DEFINED     (⍋ M LN)

      ∇ DIAGONAL[⎕] ∇
    ∇ R←DIAGONAL DIM
[1]   R←DIM⍴⍋⍋   1⊥DIM)⍴- ⍳   1↑DIM
    ∇

      ⍝ TO USE THIS FUNCTION, WE INTRODUCE THE ARGUMENT
      1 2×⍴TXT
10 20
      ⍝ WHICH, INVOKING THE FUNCTION, YIELDS A DIAGONAL
      ⍝ INDEX MATRIX  M , WHOSE UPPER LEFT PART IS
      5 5↑M←DIAGONAL 1 2×⍴TXT
  1  3  6 10 15
  2  5  9 14 20
  4  8 13 19 26
  7 12 18 25 33
 11 17 24 32 41
 16 23 31 40 50
      ⍝ BASED ON THIS INDEX MATRIX  M , THE LIST OF 1 DIGIT
      ⍝ COORDINATES ARE NOW TRANSPOSED BY A DIAGONAL ROUTE
       ⍴⎕←ITXT←,1⍉T[M]
 1 5 3 2 5 4 2 4 5 5 5 1 4 5 1 5 5 1 4 5
 1 4 1 1 2 5 1 4 5 5 2 5 5 2 5 2 5 2 5 5
 2 4 1 5 5 4 4 2 3 1 4 2 1 4 5 1 5 1 4 5
 4 1 4 5 4 2 1 1 5 2 4 4 5 4 4 4 5 2 4 1
 5 1 2 3 5 5 1 1 5 1 5 2 4 3 4 1 5 3 4 4
 2 5 5 5 4 5 2 4 2 5 4 2 3 1 2 5 5 5 2 5
 5 2 1 1 2 5 4 5 4 4 4 3 5 1 1 3 5 5 4 1
 4 2 2 1 5 1 4 4 3 5 2 4 4 5 4 1 4 2 1 4
 2 1 1 5 5 4 4 4 1 5 1 5 4 2 2 4 5 2 3 4
 4 1 3 4 5 2 4 2 5 2 5 2 4 5 2 4 1 3 1 1
10 20
```

```
      ⍝ COLUMNAR TRANSPOSITION

      ⍝ WE NOW DERIVE FROM THE KEY A NEW KEY FOR THE
      ⍝ PERMUTATION OF THE COLUMNS
      ⍴⎕←COL←(ABC GRADE KEY),(⍴KEY)+ABC GRADE (20-⍴KEY)↑KEY
7 3 5 9 14 10 2 12 6 1 8 13 4 11 17 15 16 18 20 19
20
      ⍝ THE INVERSE OF WHICH IS
      ⍴⎕←⍋COL
10 7 2 13 3 9 1 11 4 6 14 8 12 5 16 17 15 18 20 19
20

      ⍝ HENCE, BY TRANSPOSITION OF COLUMNS WE FIND
      ⍴⎕←ITXT←ITXT[;⍋COL]
 5 2 5 4 3 5 1 5 2 5 5 4 1 5 5 5 1 1 5 4
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
[illegible]
10 20

      ⍝ NOW, COMBINING THE COLUMNS, TWO AND TWO FROM LEFT TO
      ⍝ RIGHT, A MATRIX OF NEW COORDINATE PAIRS IS FORMED
      ⍴⎕←ITXT←[illegible]
[illegible] 35 15 25 54 15 55 11 54
[illegible] 15 12 15 24 52 25 52 55
[illegible] 13 24 54 42 25 15 51 54
[illegible] 45 44 52 41 44 45 42 14
[illegible] 25 55 25 31 25 15 43 44
[illegible] 52 24 55 14 24 55 25 52
[illegible] 14 54 15 15 32 35 15 14
[illegible] 55 23 42 51 54 45 14 42 41
[illegible] 14 11 21 54 24 55 45 22 43
[illegible] 24 35 45 42 52 23 41 23 11
10 10
      ⍝ BEGINNING WITH THE LEFTMOST COLUMN, WE NOW GO DOWN
      ⍝ EACH COLUMN TRANSLATING THE COORDINATE PAIRS INTO
      ⍝ LETTERS BY MEANS OF THE CHECKERBOARD
      ⍴⎕←CRPT←ABC[IABC[;ITXT]]
[illegible]
      [illegible]
100
```



```
      ⍝ THIS CRYPTOGRAM IS NOW RESHAPED INTO 5-LETTER GROUPS
      ⍴⎕←CRPT←((⌈(⍴,TXT)÷5),5)⍴CRPT
EBMGL
ERCCH
CSQAM
AIDMH
YNKSI
EMFLY
NOHRB
HCTGS
INCEI
DNBCT
CHTGV
MNCME
NEIRI
H7SDF
DINSN
DYMSQ
LEBTP
INTJF
CDCMR
EMQPL
20 5

      ⍝ IN ITS FINAL FORM, READY FOR TELEGRAPHIC TRANSMISSION,
      ⍝ IT THEREFORE LOOKS AS FOLLOWS
      4 30⍴CRPT,' '
EBMGL ERCCH CSQAM AIDMH YNKSI
EMFLY NOHRB HCTGS INCEI DNBCT
CHTGV MNCME NEIRI H7SDF DINSN
DYMSQ LEBTP INTJF CDCMR EMQPL

      ⍝ IMPLEMENTATION OF PETERSEN S RULE FOR A MATRIX OF AN
      ⍝ ODD NUMBER OF COLUMNS, IS LEFT AS A CHALLENGE TO THE
      ⍝ READER.
```

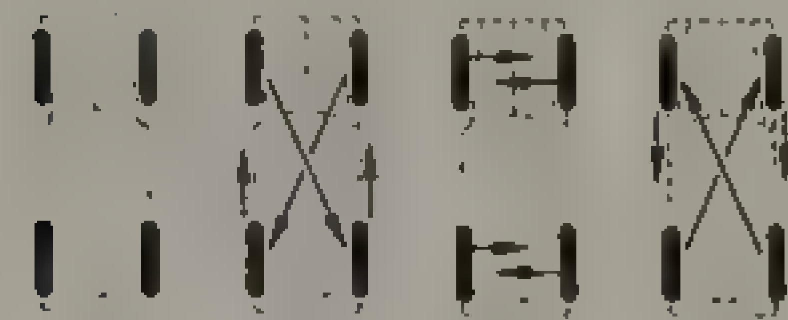
```
⍝          * * * IS IT A GROUP TABLE * * *

⍝ IF THE GROUP AXIOMS ARE STATED AS FOLLOWS
⍞←GRPAXIOMS
```

REQUIREMENT		APL EXPRESSION
LIST L & TABLE T		(1=⍴⍴L)∧2=⍴⍴T
CONFORMING DIMENSIONS		∧/(⍴L)=⍴T
CONFORMING DATA TYPES		(1↑0⍴L)=1↑0⍴T
DISTINCT ELEMENTS		∧/1=+/L∘.=L
POSTULATES	CLOSURE	∧ T∊L
	ASSOCIATIVITY	∧ T[L⍳T]=T[,L T]
	IDENTITY ELEMENT	[illegible]
	INVERSE ELEMENTS	∧/,(L∘.=L)=(T∊I)∨.∧T∊I [illegible]
	COMMUTATIVITY	∧/,T=⍉T

```
⍝ THEN WE NOTE THAT IT IS
CLGRPAXIOMS
AN ORDERED TABLE OF GROUP AXIOMS.  TO PRODUCE THE APL
EXPRESSIONS WITHOUT HEADINGS ETC., WRITE IN 1-ORIGIN
GRPAXIOMS[(5+⍳4),11 13 15 17 18 20,36+⍳22]

⍝ TEST PROCEDURE

⍝ ASSUME 1-ORIGIN
⎕IO←1
⍝ THEN A CHARACTER MATRIX OF THE ORDERED TESTS ARE
[illegible]
[illegible]
[illegible]
(1↑0⍴L)=1↑0⍴T
∧/1=+/L∘.=L
∧/ T∊L
∧/,T[L⍳T;]=T[;L⍳T]
I←⍴I←((T∧.=L)∧L∧.=T)/L
∧/,(L∘.=L)=(T∊I)∨.∧T∊I
[illegible]
[illegible]
10 22

⍝ HENCE, BY EXECUTING THIS MATRIX ROWWISE, THE GIVEN
⍝ DATA MAY BE TESTED FOR ALGEBRAIC STRUCTURE, IF ONLY
⍝ THESE DATA ARE ASSIGNED TO THE VARIABLES  L  AND  T
```



```
⍝          * * * IS IT A GROUP TABLE * * *

⍝ DATA PREPARATION

⍝ CONSIDERING OUR FAVOURITE AUTOMOBILE EXAMPLE
```




```
⍝ THE CARRIER OF STRATEGIES IS
⍞←L
EABC
4

⍝ WHILE THE MULTIPLICATION TABLE IS
⍞←T
EABC
ABCE
BCEA
CEAB
4 4

⍝ TESTS ON DATA DEFINITION

⍝ WE HAVE HERE FOUR REQUIREMENTS TO BE SATISFIED.
⍝       1) THE VECTOR MATRIX RANK REQUIREMENTS
⍎⍞←GRP[1;]
(1=⍴⍴L)∧2=⍴⍴T
1
⍝       2) CONFORMING DIMENSIONS
⍎⍞←GRP[2;]
∧/(⍴L)=⍴T
1
⍝       3) CONFORMING DATA TYPES (CHARACTER OR NUMERIC)
⍎⍞←GRP[3;]
(1↑0⍴L)=1↑0⍴T
1
⍝       4) NON-REPEATED ELEMENTS IN THE CARRIER
⍎⍞←GRP[4;]
∧/1=+/L∘.=L
1
```

```
⍝          * * * IS IT A GROUP TABLE * * *

⍝ BY VISUAL INSPECTION WE FURTHER VERIFY THAT THE ORDER
⍝ OF THE FIRST ROW AND COLUMN OF  T , AGREE WITH THAT OF
⍝ THE CARRIER  L .

⍝ IT IS THEREFORE CONCLUDED THAT THE DATA DEFINITION IS
⍝ SATISFACTORY, SO THAT WE MAY PROCEED WITH THE PROPER
⍝ AXIOM TESTS


⍝ CLOSURE

⍝ THE TABLE HAS THE STRUCTURE OF A  GROUPOID , SINCE
⍎⎕←GRP[5;]
  ∧/,T∊L
1


⍝ ASSOCIATIVITY

⍝ THE ALGEBRAIC STRUCTURE PROVES TO BE A  SEMIGROUP
⍎⎕←GRP[6;]
 ∧/,T[L⍳T;]=T[;L⍳T]
1


⍝ IDENTITY LAW

⍝ THE STRUCTURE IS A  MONOID  SINCE PRECISELY ONE ROW
⍝ AND ONE COLUMN OF TABLE 'T' ARE REPLICAS OF  L
T∧.=L
1 0 0 0
L∧.=T
1 0 0 0
⍝ OR, COMBINING THESE TWO TESTS INTO ONE WHICH AT THE
⍝ SAME TIME DETERMINES THE IDENTITY ELEMENT
⍎⎕←GRP[7;]
1 ρI←((T∧.=L)∧L∧.=T)/L
1
⍝ THAT IS, THE IDENTITY OR NEUTRAL ELEMENT IS
I
E


⍝ INVERSE LAW

⍝ FIRST, SINCE BY THIS LAW EVERY ELEMENT HAS AN UNIQUE
⍝ INVERSE, THE IDENTITY ELEMENT  I  MUST APPEAR EXACTLY
⍝ ONCE IN EACH ROW AND COLUMN
[illegible]
1
⍝ SECONDLY, SINCE BY THE INVERSE LAW ELEMENT  X  AND ITS
⍝ INVERSE ELEMENT  X  COMMUTE, THE POSITIONS OF  I  MUST
⍝ BE SYMMETRICAL ABOUT THE PRINCIPAL DIAGONAL
∧/,(T∊I)=⍉T∊I
1
```



```
⍝          * * * IS IT A GROUP TABLE * * *

⍝ COMBINING THESE TWO CONDITIONS, WE SEE THAT THE MATRIX
⎕←T∊I
 1 0 0 0
 0 0 0 1
 0 0 1 0
 0 1 0 0
4 4
⍝ MUST BE A SYMMETRICAL PERMUTATION MATRIX
⍎⎕←GRP[8;]
[illegible]
1
⍝ HENCE, THE ALGEBRAIC STRUCTURE IS A  GROUP .

⍝ THE INVERSE ELEMENTS MAY NOW BE ORDERED IN A VECTOR  L
⍎⎕←⍎⎕←GRP[9;]
 L←L[(ρL)|+/T∊I]
ECBA
4
⍝ AS DEFINED BY THE ORDERING OF THE CARRIER
L
EABC

⍝ SINCE BY COMPARISON OF  L  AND  L  WE SEE THAT ELEMENT
⍝  B  IS ITS OWN INVERSE, THE MULTIPLICATION TABLE  T
⍝ CONTAINS A SUBGROUP DEFINED BY ELEMENTS  E  AND  B
T[L⍳'EB';L⍳'EB']
EB
BE


⍝ COMMUTATIVITY

⍝ SINCE THE TABLE IS SYMMETRICAL ABOUT THE PRINCIPAL
⍝ DIAGONAL (FROM UPPER LEFT TO LOWER RIGHT)
⍎⎕←GRP[10;]
 ∧/,T=⍉T
1
⍝ THE GROUP IS CLEARLY  COMMUTATIVE  OR  ABELIAN .

⍝ THE POSSIBILITY OF DIVISION

⍝ IT MAY AMUSE THE READER TO INVESTIGATE ALTERNATIVE
⍝ AXIOM SYSTEMS SUCH AS COMBINING THE IDENTITY AND
⍝ INVERSE LAW INTO A SINGLE POSTULATE DEMANDING A
⍝  UNIQUE SOLUTION OF ANY GROUP EQUATION .

⍝ THIS ALTERNATIVE PROPERTY IMPLIES THAT THE TABLE
⍝ IS A  LATIN SQUARE . THAT IS, EACH COLUMN AND EACH
⍝ ROW OF  T  MUST BE A PERMUTATION OF  L .
```

A Conservation Law of the Message

3.1 Language is Pattern

The classical way of breaking a simple or monoalphabetic substitution cipher, is simply to guess a word or fraction hereof and explore the consequences. An illuminating quotation by de Vigenère in this respect, is found in one of the footnotes to Lindenfels' book, published in 1819. [1]) In the quotation which follows, the name Bayard is casually mentioned. To the contemporary reader, this remark gave away the social status of Vigenère, for Bayard was the most famous knight in Europe even if he was captured by Henry VIII in August 1513 at the Battle of the Spurs, so called because of the rapidity of the French retreat. Anyhow, in 1587 Vigenère said:

> "*Everyone may devise cyphers to his fancy, and alphabets too, in one way or another and more or less artificial and ingenious, according to his knowledge. In agreement with the deftness of mind, some cyphers arrived at are more instructive than others. Yet, the mainpart of those which I have seen used at the courts of princes, consists solely in a multiplication of characters made to please. Esteemed by being bizarre, unknown, and in great number, they cannot convey meaning without communicating the alphabet. For the vowels, because they are far more frequent than other letters, will appear three to four times more often. The rest will be of equal significance together with the doubles, the nulls, and the everywhere peculiar signs, each designating a word such as emperor, king, arms, provisions, the Gauls* [the French], *and similar others. Still all this does not get the better of men, penetrating into the secret by ingenuity and vivid conjectures, albeit also by extreme intellectual effort and incomprehensible mental fatique*
>
> *Thus, I recall having seen in my youth while being employed by General Bayard, the secretary of state of the great King François, the late Monsieur Bourdaisiere, grandfather of those living today, as he often decyphered, without alphabet to match, several intercepted despatches in Spanish, Italian, and German, of which he understood nothing or very little. With perseverance he worked continually on it day and night for three weeks, first then being able to deduce a single word. Yet, with this first breach accomplished, all the rest came tumbling down, just like demolishing a wall. ... Why this can be accomplished, is that there are certain secrets and maximes; like the frequency*

[of occurrence] *grading the letters; their sequence and concomitance; and other such ingenious considerations and rules, and I know not what, that they have in common with anagrams and reversed names, in which respect some are more successful than others. Indeed, all encyphered writings put together, are almost nothing else but anagrams, if we consider the few letters which, by their various transpositions and assemblies, can express for ever all different meanings: reduced to begin with to syllables; then the syllables into expressions; and these expressions finally weaved into statements, and complete speech. Such deftness, and on top conjectures expressing the human spirit, finally lead to the crude cyphers, and to their discovery".*

This description fits Babbage's cryptographical accomplishments too. Yet, Babbage was also the man who declared, in his *The Exposition of 1851*, that: "*It is not a bad definition of man to describe him as a tool-making animal*". [2]) So, true to this belief, he started making tools for deciphering. One of these tools, a code-breaker's dictionary in English, was to form a major part of his proposed book on deciphering. This, it may be recalled, is one of the few facts Babbage ever disclosed about his intentions. Thus, he wrote (see figure 9):

> "*I have prepared extensive lists of all words of English language arranged in classes as material on the philosophy of decyphering to which, on rare occasions, I give half an hour as relaxation from my daily labour*"

The work on this project was on a grand scale, and continued for years. "*Any member of the family was liable to be roped in*", as Hyman recounts. [3]) Of course, like so many of Babbage's brilliant undertakings, it was never finished. Even more sad, whatever work there was done, the manuscripts have been lost. For, as L. H. Dudley Buxton, a grandson of Babbage's close friend H. W. Buxton, remarked in 1933: [4])

> "*Like so many mathematicians, he was keenly interested in ciphers and published one or two papers on the subject; at the same time, he amused himself with anagrams and other kindred matters. This led him to compose a dictionary which unfortunately has not survived as far as I am aware; words were arranged according to the number of letters it contained, an invaluable aid it would appear to solvers of cross-word puzzles!*"

Possibly, the manuscripts were among the items withdrawn by the family from Babbage's library, before it was put on sale after his death. Babbage passed on his interest in ciphers to the younger generation of his family, such as his nephew Henry, or his niece Louise, so possibly one of them inherited his dictionary. [5]) I much doubt that the manuscripts went to his youngest son Henry, because he donated Babbage's cryptographical files to British Museum.

We may imagine that Babbage was inspired to the task by his work on Bishop Wilkins' universal language. Yet, it took an entirely different direction which, in his autobiographical *Passages*, he described as follows: [5])

> "*One great aid in deciphering is, a complete analysis of the language in which the cipher is written. For this purpose I took a good English dictionary, and had it copied out into a series of twenty-four* [twenty-six?] *other dictionaries. They comprised all words of*
>
> *One letter,*
> *Two letters,*
> *Three letters,*
> *&c. &c.*
> *Twenty-six letters.*
>
> *Each dictionary was then carefully examined, and all the modifications of each word, as, for instance, the plurals of substantives, the comparatives and superlatives of adjectives, the tenses and participles of verbs, &c., were carefully indicated. A second edition of these twenty-six dictionaries was then made, including these new derivatives.*
>
> *Each of these dictionaries was then examined, and every word which contained any two or more letters of the same kind was carefully marked. Thus, against the word* tell *the numbers 3 and 4 were placed to indicate that the third and fourth letters are identical. Similarly, the word* better *was followed by the numbers 25, 34. Each of these dictionaries was then rearranged thus: – In the first or original one each word was arranged according to the alphabetical order of its initial letter.*
>
> *In the next the words were arranged alphabetically according to the* second *letter of each word, and so in the other dictionaries on to the last letter.*
>
> *Again, each dictionary was divided into several others, according to the numerical characteristics placed at the end of each word. Many words appeared repeatedly in several of these subdivisions.*
>
> *The work is yet unfinished, although the classification already amounts, I believe, to nearly half a million words*
>
> *From some of these, dictionaries were made of those words only which by transposition of their letters formed anagrams*".

To which description Babbage added a list of the latter kind which he found "*curious*" by their twist of content of meaning, such as,

Opposite:	*vote – veto;*	*fowl – wolf;*
Similarity:	*note – tone;*	*cold – clod,*
Satirical:	*bard – drab;*	*tame – mate*

Example of the Utility of Dictionaries
of Characteristic Words

18 Aug 1857

Dined in Park Lane – Sir John H. Storks, Ld Panmure, Capt Drummond, The Turkish Ambassador Mohammed

Conversation about cypher with Genl Sir H Storks. Afterwards Ld Panmure joined in. Sir H. S mentioned a dispatch he had recd when in the East Constantinople perhaps from Ld P[almerstone] *(in cypher per Elec telegraph) respecting the return of certain regiments to India, which in translation were "send some". The dispatch was immediately answered by a statement that it would be the certain destruction of many of the men if they were sent in that season*

Sir H. Storks having just returned this answer took a ride and after a time it occurred to him that some mistake must have occurred in the transmission of the message. He therefore returned and telegraphed each station in succession to repeat that portion [of] *the words "send some". All concurred until post trans past the telegraph repeated the words "send* none*" which explained the affair.*

Figure 41. Babbage's note on the garbled message
(BL, Add.Ms. 37205, F. 196)

Anyhow, as one can see, it was no mean job to carry out this project. We also begin to understand, how unusual his book on deciphering would have been, had he published this material. In fact, Babbage's dictionaries were so comprehensive that only the modern computer has made it economically feasible to publish word lists competitive in size. [6])

Ostensibly designed as a general tool of deciphering, the dictionaries are merely explained in his *Passages* as an expedience to "*some verbal puzzles costing much time to solve*". One such kind of puzzle considered by Babbage, is the development of anagrams such as turning the sentence: "*Art is not in, but Satan*" into the eighteen-letter word "*transubstantiation*". Another type, is what Babbage calls "*squaring words*". For instance, to square the word "*Dean*", Babbage writes it in the first row and column of a table, filling up the rest of the table "*with such letters that each vertical column shall be the same as its corresponding horizontal column, thus*"

```
D e a n          D e a n
e . . .    =>    e a s e
a . . .          a s k s
n . . .          n e s t
```

Babbage's cryptographical file in the British Library contains only a single reference to the dictionaries, namely the note transcribed in figure 41. Undoubtedly, he jotted it down before he went to bed that night in mid-August 1857. From its heading, we may infer that he intended to include the anecdote in his *Philosophy of*

Deciphering. Possibly, this is the last item he collected for his book. The letter, telling that he had to give up this work for the time being, was dated early in December that same year.

Apart from this note, his cryptographical manuscripts do not reveal to what extent he relied on the dictionaries. However, I believe it to be a general observation that he always seized on the word divisions, in order to make his initial breach into a cipher by guessing a probable word. If the message was a letter, he would concentrate on standard phraseology in the opening or closing sentences. Otherwise, he would focus on the short words of one, two, or three letters aided by a letter frequency count. Several times, we find a spate of such words poured over his worksheets. Perhaps they were copied from the dictionaries.

An important clue to the guessing of words and letters, is the identification of the word patterns of vowels and consonants. [7]) It is thought-provoking that our conventional notation of mathematical expressions, using letters to denote the known and unknown entities, was inspired by such techniques of deciphering. Thus, this tradition began with François Viète who in his *In artem analyticam Isagoge*, published in Tours 1591, introduced vowels for the designation of unknown quantities and consonants for the designation of known quantities. In translation from Latin, his words are: [8])

> *"That this work may be aided by a certain artifice, given magnitudes are to be distinguished from the uncertain required ones by a symbolism, uniform and always readily seen, as is possible by designating the required quantities by letter A or by other vowel letters E, I, O, U, Y, and the given ones by the letters B, G, D or by other consonants".*

The modern practice of using the last letters, *X, Y, Z* of the alphabet to denote the unknowns, and the first letters: *A, B, C* to denote the knowns, was introduced by René Descartes in his *La Géométrie*, published 1637. In our APL terminal sessions, we live up to this tradition by denoting the known plaintext alphabet "*ABC*", and the unknown cipher alphabets "*XYZ*" or "*PQR*", as needs be.

However, to appreciate the connection between cryptography and today's standard practice in mathematical notation, it is necessary to know that Viète in his day was equally famous as a mathematician and as a cryptographer. An interesting account hereof has been given by Joseph Fourier, the great mathematical physicist whom Babbage, in his *Passages*, counted "*amongst my earliest friends in Paris*". Fourier published his biography of Viète anonymously in 1827, signing himself "Z", together with a biography of another great mathematician and cryptographer, John Wallis, which he signed "*F J.*". [9]) Babbage's description in his *Passages* would seem to suggest that his strongest memories of Fourier relate to his visit in Paris in 1826 together with his wife Georgiana. This fits the time of writing of Fourier's two

biographies. So, perhaps a chance remark on secret writing during their conversation inspired Fourier to look into the strange relationship between the process of mathematical discovery and that of deciphering. But, let Fourier himself recount:

> *"Since the Spaniards could not prevent the interception of their communication among the separate members of their vast monarchy, they had invented a convention of writing, which they even varied from time to time in order to thwart all those trying to track their correspondence. This cypher, composed of more than fifty signs, served them excellently during our civil wars.*
> *Viète, having been assigned by the King to find the key, easily succeeded and discovered even a means for following all variations. France profited for two years by this discovery. The Spanish Court, baffled, accused that of France of having employed the devil and sorcery. After their complaint to Rome, Viète was summoned as a necromancer and a sorcerer. This aroused much laughter".*

Like Babbage, Viète undoubtedly explored the inherent weaknesses of the ciphers, as well as the cryptographical ignorance or even sheer carelessness of the correspondents using them. In his book from 1819, Lindenfels devotes the better part of a chapter to the latter question. Among the precautions which he recommends the correspondent to observe, the following are representative: Use false or no word divisions (or, as we would say today, use a *formal* division into 5-letter groups); begin and end with a series of nulls forming *"des mots perdue"* ("empty" words); make sure that no repeated word is enciphered in the same way; drop punctuation marks and accents; spell out special vowels (in Danish, for example, substitute "Ø" by "OE" or, in APL, by "Q", which looks almost the same); agree to abbreviations and to deviations from orthographic standards; mix languages and, if a cryptogram is enclosed with a plaintext, never write the two in the same language.

Clearly, the attendance to such details on the part of the correspondents, makes it necessary to come up with new cryptographical tools and to sharpen those already in use. In particular, we have to go beneath the level of the probable word and consider frequent letter combinations instead, from that of a single letter and upwards. Technically, since the Greek word for letter is *gramma*, these combinations of one, two, three, etc. letters are denoted: *monogram, digram, trigram, tetragram, pentagram, hexagram*, etc.; or in general, *polygram*. In APL, however, we shall find it convenient to use the term *Ngram* to designate the last mentioned general case. The point here, is that the frequency of occurrence of the letters and their combinations, are subordinate to statistical patterns characteristic of the language and of the content of the messages.

Of course, if man puts his mind to it, he may destroy this pattern, although usually at the cost of introducing another. The following lines, written in the tradition of old Norse poetry with its fondness for alliteration, may illustrate this aspect. A contemporary of Babbage's, Miss Kitty Stephens was a celebrated London vocalist, later to become the Countess of Essex. Incidentally, this description of her art is also an *acrostic*, since the first column of letters forms her name:

S he sings so soft, so sweet, so soothing still
T hat to the tone ten thousand thoughts there thrill,
E lysian ecstasies enchant each ear –
P leasure's pure pinions poise — prince, peasant, peer,
H ushing high hymns, Heaven hears her harmony, –
E arth's envy ends; enthralled each ear, each eye;
N umbers need ninefold nerve, or nearly name,
S oul-stirring Stephens' *skill, sure seraphs sing the same.*

Among the statistically more extreme cases, are the *lipogrammatists*, purposely dropping one or more letters, and the *pangrammatists*, crowding all the letters of the alphabet into every verse or into a single line. A curious example of the former, is a story written in 1824 by Lord Holland, in which all the vowels except the letter "E" was omitted. Entitled *"Eve's Legend"*, it was concluded by the words: *"Here endeth the legend"*. Augustus de Morgan, in his *A Budget of Paradoxes*, puts himself in the latter class by telling that he and his colleague William Whewell once amused themselves by trying to write sentences that used all the letters of the alphabet once and once only. One example that comes close to the ideal, is: *"Get nymph, quiz sad brow; fix luck"*, which de Morgan explains as good advice to a young man. *"Marry be cheerful; watch your business"*.

Anyhow, in more ordinary communication such extreme cases are exceptional. Thus, it is well known that when Samuel F. B. Morse in 1838 devised what we now know as the Morse code, representing the alphabet by spaces, dots and dashes, he estimated the relative frequencies of occurrence of the various letters by counting the number of types in the different compartments of a printer's type box. Thus, since the letter "E" was the most frequent type, it was assigned the shortest possible code symbol, namely a single dot.

It is rather strange that neither was Morse's choice guided by tables of the relative frequencies of various letters in English text, nor were letters in text counted to get such data. The more so, since such data were published in scientific journals such as the *Correspondance mathématique et physique*, edited by Babbage's Belgian friend, the statistician Lambert Adolphe Jacques Quetelet, whom Babbage met at a dinner in Paris in 1826, where he went together with his wife Georgiana.

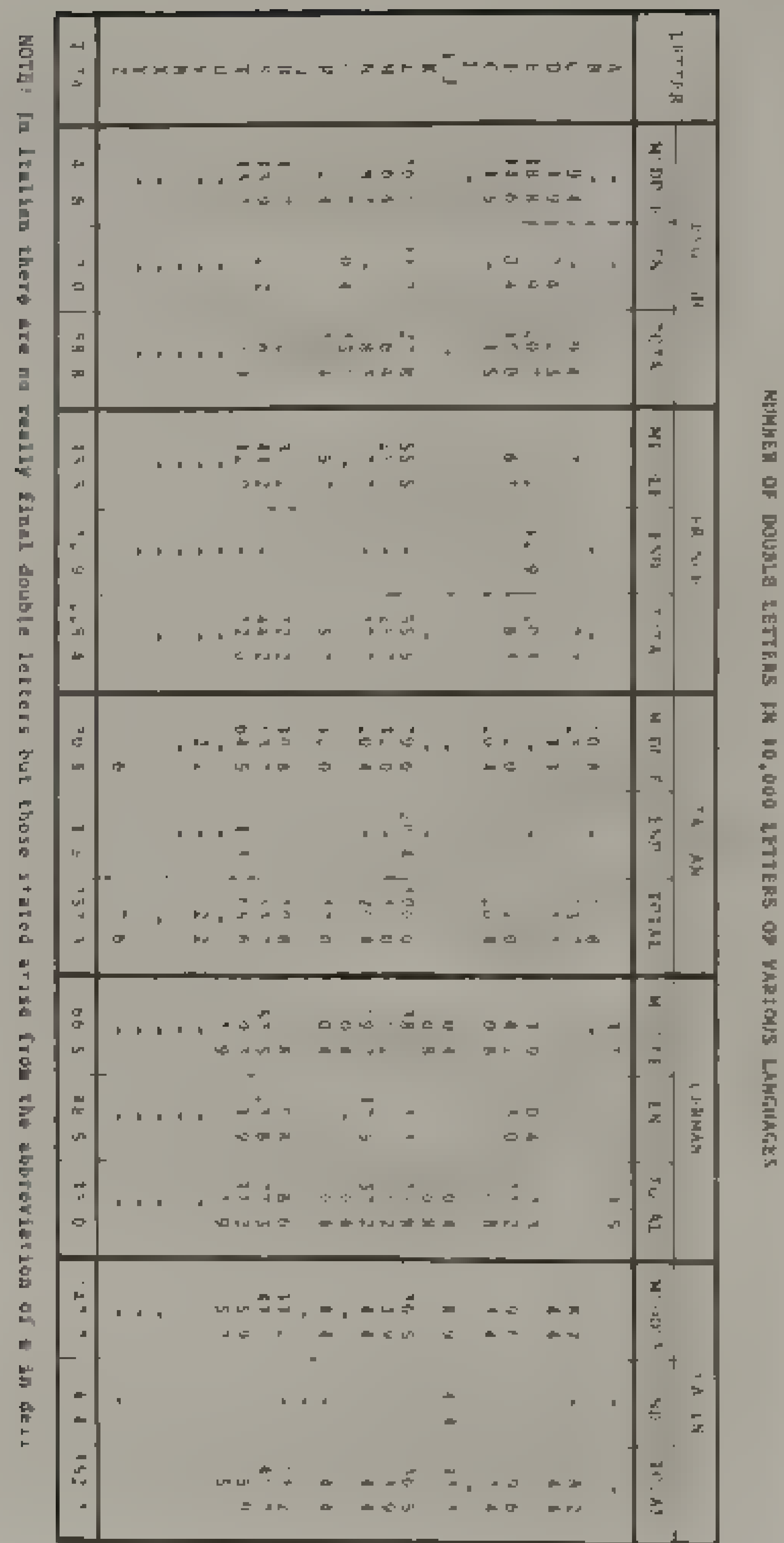


Figure 42. Babbage's count of double letters. (BL, Add Ms. 37205, F. 230)

One of the contributions on this topic in Quetelet's publication was a letter from Babbage which Quetelet translated into French and published in 1831. [10]) Never printed in English, its title was given as: "*On the Proportion of Letters Occurring in Various Languages*" in Babbage's list of publications.

The essence of this paper, or letter to the editor, is a table of relative frequencies of occurrence of double letters in various languages. A handwritten original of this table, which I found among Babbage's cryptographical manuscripts in the British Library, is transcribed in figure 42. The heading and the note are Babbage's own formulations. In the published version, only the first column is given for each language, while the numbers in the middle column are incorporated into the text. Quetelet must have been in quite a hurry, for he says that the count is based on 10,000 *words* where Babbage has 10,000 *letters*. Also Quetelet has overlooked a serious printer's error in the published version, displacing the entire column for the German language. There are also several misprints in the other entries.

The paper itself falls in three parts. First, it refers to previous contributions in the journal on the same topic by other authors. It then continues with a brief explanation of the contents of the table. It concludes by giving the numbers not in the printed table, ending with the remark:

> *"Mr. Babbage suggests, as objects for analogous researches, the formation of tables for words of two letters and the estimation of the number of times each of them appears in 10,000 words. One can also do the same research for words of three letters".*

Although the table was published in 1831, it and its associated material are not placed chronologically among the contemporary manuscripts in Babbage's cryptographical file in the British Library. On the contrary, it would appear that this material has been moved to be put together with similar statistical material, which can be dated to the period in 1858, when Babbage was busy with the ciphers of Charles I and Henrietta Maria, and the planning of his book on the *Philosophy of Deciphering*. Only Babbage himself could have done this. There can be little doubt, therefore, that Babbage was extending and preparing this material for publication in his book.

A remark: "*Heinrich Phosphorescences Vol. 1 & 2*" added to the table in pencil, reveals by comparison with Tucker's catalogue of Babbage's library, that Babbage did his count on the German language using a two-volume work, Heinrich (Placidus): *Die Phosphorescenz der Körper*, published in Nürnberg, 1811-15. In a note, Tucker describes this book as, "*A very important work, in which the author has explained the phenomena of light emanating from bodies shining in the dark*".

It is also evident from Babbage's various other notes in this material that he extended the English contents in the table by counts of the relative frequencies of

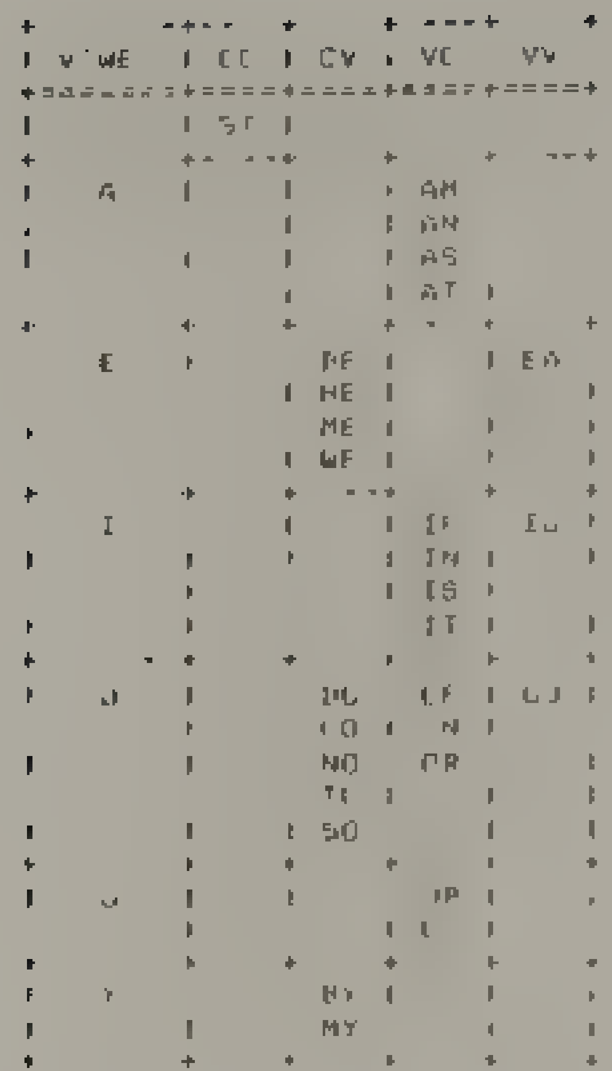


Figure 43. Two-letter words by C/V pattern

occurrence of single letters, of what he calls *penultima* letters (i.e., letters next to the last syllable in a word), and of two- and three-letter words. To this end, he consulted the first seventeen pages of what he refers to as "*Blair's Sermons, Vol. I*". These sermons by Hugh Blair (1718-1800), a professor of theology at the University of Edinburgh, were published in five volumes over the period 1777-1801. [11])

Simultaneously with this statistical work, Babbage started to write new word lists on the *consonant/vowel patterns*, the so-called "*C/V patterns*", of words of two, three, four, and five letters. For example, considering 3-letter words, he began to organize lists according to patterns such as: CCV, VCC, CVC, VCV, CVV, VVC, and VVV (folios 248-249); and he made lists of 3-letter words according to whether they were "*most frequent*" or "*less frequent*" (folio 246). He also commenced to order various words ending on "*ion*" according to word length. Figure 43 extends his ideas by also organizing the two-letter words according to the vowel identity. The pairs of vowels in this figure are those most frequently met with in words of three or more letters.

Statistics was to Babbage a dominating interest, and he published several papers on the subject. He did considerable research on actuarial tables of life expectancy,

and his book on this subject, *A Comparative View of the Various Institutions for the Assurance of Lives*, published in 1825, was translated into German. It was at a meeting in his home in 1834, that the plan was contrived which in the same year led to the formation of the *Statistical Society*. Whatever he contributed, it was central to the topic area.

Yet, if we examine various books on cryptography, none of them exhibits any particular interest in the frequencies of occurrence of double letters. Indeed, if such counts are given at all, it is always as part of a general digram count. Why Babbage became so absorbed in this, apparently esoteric, topic is not known. Still, the course of events again proved his intuition right. For in 1922, William Frederick Friedman introduced the frequency of occurrence of a pair of identical letters as the basic statistical measure, marrying cryptography to mathematical statistics. This measure of double letters was Friedman's famous *Index of Coincidence*, opening up for a wealth of new statistical techniques in codebreaking.

One of the most famous codebreakers in our time, Friedman promoted the establishment of punch card installations in the 1930s at Pearl Harbour, Corregidor, and Washington. During World War II, this development was followed up by the building of special-purpose, all-electronic computers. Also, in a dramatic application of his methods, his team painstakingly broke the most secret and complex Japanese cipher, known as *PURPLE*, by constructing a duplicate of the rotor mechanism that produced it. [12])

Friedman's original tests were revised, and their area of application expanded, in 1935 by Solomon Kullback, one of Friedman's colleagues and former "students". [13]) Figures 44 A and B give the mathematical background and establish the necessary APL-functions for a more elementary of these applications, namely the determination of whether a given frequency count reflects a monoalphabetic or a polyalphabetic encipherment. This method, known as the *phitest*, is instructive for the elegant simplicity with which it brings the basic notion of statistical independence to bear on an important cryptographical problem. [14])

3.2. I. B. Lindenfels, a Major in Frederik VI's Army

In 1918, Charles J. Mendelsohn was made a Captain in the Military Intelligence Division of the General Staff of the U. S. Army, in charge of decipherment of German codes. A classic scholar and faculty member of the history department in the College of the City of New York, he was launched by this experience into a lifelong study of historical ciphers and their originators. Among other things, this research resulted in two fundamental papers on Cardano and de Vigenère, respectively. The latter appeared in 1940, [15]) a year after Mendelsohn's death on 27

```
FOR THE LETTERS OF ALPHABET  ABC    LET THERE BE SPECIFIED
TWO DISTRIBUTIONS OF FREQUENCIES OF OCCURRENCE,
      THE EXPECTED    FRQ ,  FOR A SAMPLE PLAINTEXT
      THE OBSERVED    DST ,  FOR A GIVEN CRYPTOGRAM

                THE INDEX OF COINCIDENCE

TWO HYPOTHESES ARE PROPOSED ABOUT THE DISTRIBUTION   DST
    (1) IT IS A RANDOM DISTRIBUTION (EQUAL PROBABILITY
        OF ALL LETTERS IN  ABC )  IDEALLY PRODUCED BY A
        POLYALPHABETIC SUBSTITUTION,
    (2) IT AGREES WITH THE EXPECTED DISTRIBUTION,  FRQ ,
        AND SO STEMS FROM A MONOALPHABETIC SUBSTITUTION.

THE STATISTICAL MEASURE,  USED TO VERIFY OR REFUTE THESE
HYPOTHESES,  IS THE PROBABILITY THAT ANY TWO LETTERS
SELECTED AT RANDOM WILL COINCIDE (OR BE IDENTICAL). THUS,
FOR THE TWO HYPOTHESES THE EXPECTED VALUES ARE DETERMINED

                  ∇ KAPPA[⎕] ∇
                ∇ K←ABC KAPPA FRQ,KR,KP
           [1]  RANDOM KR←1÷⍴ABC
           [2]  PLAIN KP←+/FRQ*2
           [3]   K←KR,KP
                ∇

THE DESIGNATIONS   KR  AND  KP   REFLECT FRIEDMAN'S CHOICE
OF THE GREEK LETTER   KAPPA  TO DESIGNATE THE TWO INDICES,
WITH SUBSCRIPTS  R  FOR RANDOM AND  P  FOR PLAINTEXT.

RANDOM TEXT   WITH EQUIPROBABILITY OF ALL  ⍴ABC  LETTERS,
THE PROBABILITY OF A SINGLE LETTER IS    1÷⍴ABC    AND OF
A PAIR OF LETTERS    (1÷⍴ABC)*2 .   HENCE, FOR ALL   ⍴ABC
PAIRS THE PROBABILITY IS    (⍴ABC)×(1÷⍴ABC)*2 ,  OR   KR .

PLAINTEXT   THE PROBABILITY OF A SINGLE LETTER, SAY   X ,
IS    FRQ[ABC⍳'X'] ,  AND OF A PAIR OF IDENTICAL LETTERS
 FRQ[ABC⍳'X']*2 ,  SINCE THE OCCURRENCE OF A PAIR OF ONE
LETTER AND THE OCCURRENCE OF A PAIR OF ANOTHER LETTER, ARE
[illegible] EXCLUSIVE EVENTS, THE PROBABILITY OF
ONE OR THE OTHER IS THE SUM OF THEIR PROBABILITIES, OR  KP .

                COINCIDENCES IN ENGLISH

THE EXPECTED DISTRIBUTION   FRQ   FOR THE  26 ⍴ABC  LETTERS
IN ALPHABETICAL ORDER, IS FOR ENGLISH PLAINTEXTS

0.0805 0.0162 0.032  0.0365 0.1231 0.0228 0.0161 0.0514 0.0718
0.001  0.0052 0.0403 0.0225 0.0719 0.0794 0.0229 0.002  0.0603
0.0659 0.0959 0.031  0.0093 0.0203 0.002  0.0188 0.0009

HENCE, THE INDICES OF COINCIDENCE ARE
            ABC KAPPA FRQ                 ÷/⌽ABC KAPPA FRQ
      0.0385 0.066                   1.72
WHERE A RATIO OF  1.72  EXPLAINS WHY THEY CAN BE DISCERNED.
```


Figure 44 A. The index of coincidence and the phitest.

```
IT IS A WELL KNOWN FACT,  DEMONSTRATED IN ANY MATHEMATICS
TEXTBOOK  THAT THE NUMBER OF COMBINATIONS OF  N  DIFFERENT
THINGS TAKEN  R(≤N)  AT A TIME IS
    (!N)÷(!R)×!N-R    AND THUS   (N×N-1)÷2   FOR  R = 2

                      THE PHITEST

SINCE THE OBSERVED DISTRIBUTION IS BASED ON A TOTAL NUMBER
OF LETTERS    N←+/DST    THEN THERE IS POSSIBLE A TOTAL OF
 (N×N-1)÷2   PAIRS.   HENCE, MULTIPLICATION OF   KR   AND
 KP  BY THIS NUMBER  WILL SCALE THEM FOR THIS DISTRIBUTION

SIMILARLY, IF LETTER   X   OCCURS   DST[ABC⍳'X']   TIMES,
IT IS EQUIVALENT TO   (DST[ABC⍳'X'] × DST[ABC⍳'X'] - 1)÷2
COINCIDENCES.

THE PHITEST COMBINES THESE RESULTS

                  ∇ PHITEST[⎕] ∇
                ∇ R←FRQ PHITEST DST
           [1]  ASSUME →((⍴ABC)≠⍴FRQ)/0
           [2]  COINCIDENCE R←ABC KAPPA FRQ
           [3]   [illegible]
           [4]  OBSERVED R←0.5×R,+/DST×DST-1
                ∇

                ILLUSTRATIVE APPLICATIONS

A CRYPTOGRAM IN THE TIMES, 21 SEP. 1854, STATES

 THIRTEEN -
 YLVZ-ALHEZA-AHVDOLY'-ZUSJD KLHXLYZ MHG B BHF-YZBE -YHFL
  GJ FHAD [illegible]

THE FREQUENCY DISTRIBUTION   DST1 ,  OMITTING LINE 1, IS
   3 5 0 1 5 9 4 7 1 1 2 12 1 2 2 0 0 0 3 0 7 2 0 4 9 7
SINCE
                  FRQ PHITEST DST1
          143 88 246 84 243
THE CIPHER IS MONOALPHABETICALLY ENCIPHERED.


ANOTHER CRYPTOGRAM IN THE TIMES, 21 JULY 1854, READS

          OZZES, OV, TNSRXWVFJO. LXWV, OHOJZ,
          FXHFJBX  QXNOZFD  RHAD [illegible]
          XY, DUOB, SLUP, TAUB, VJPTGRSIW, JTZ,
          SD, EJPLMOFF, ZUGOSCG  -  VRBV.

THE CORRESPONDING FREQUENCY DISTRIBUTION,  DST2 , IS
   1 0 1 3 3 7 5 1 1 5 0 3 2 2 0 3 4 4 7 5 5 6 3 7 2 6
SINCE
                  FRQ PHITEST DST2
          198.12 339.88 219
THE CIPHER IS POLIALPHABETICALLY ENCIPHERED.
```

Figure 44 B. The index of coincidence and the phitest.

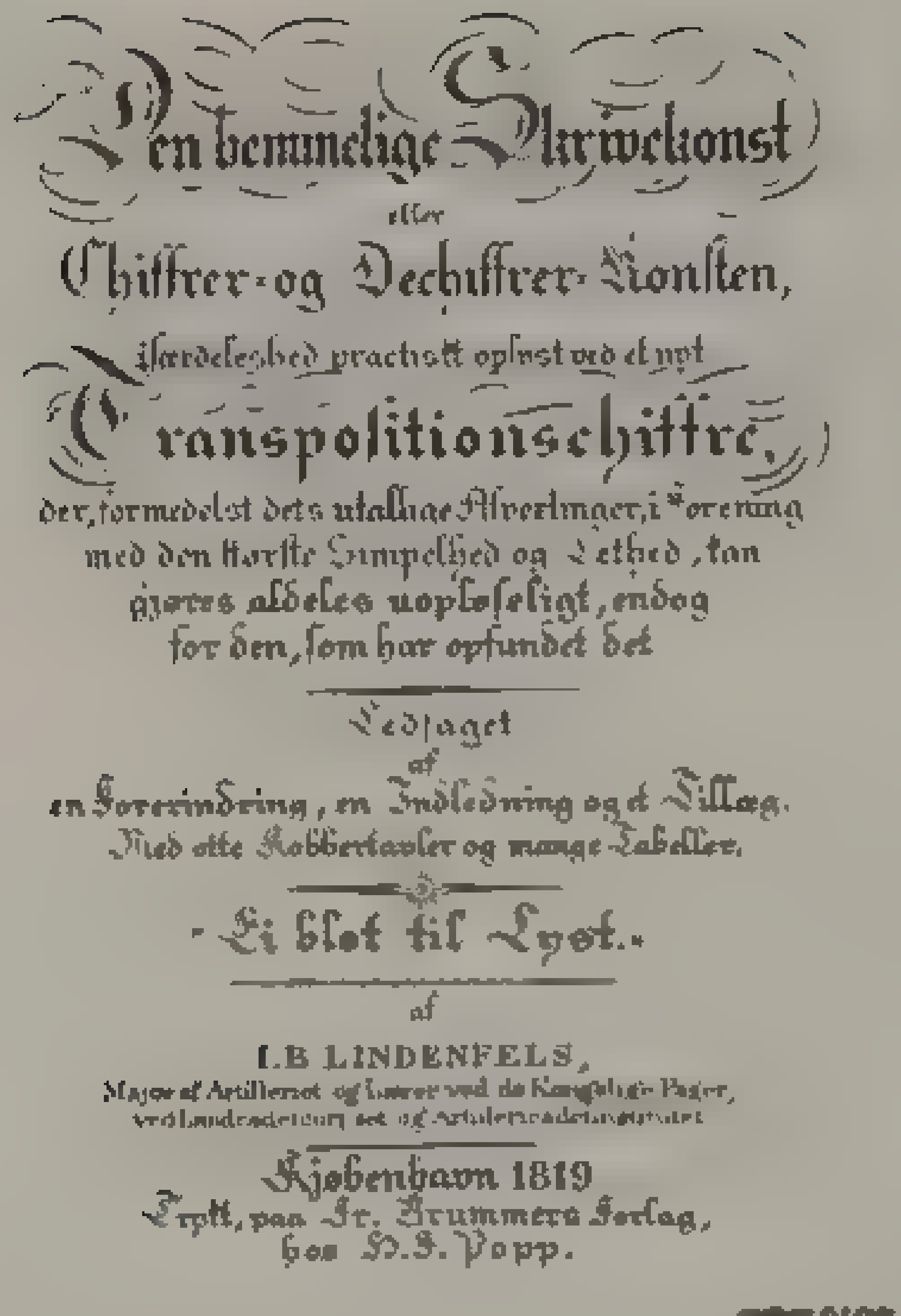

Den hemmelige Skrivekonst
eller
Chiffrer- og Dechiffrer-Konsten,
især deles hed practiskt oplyst ved et nyt
Transpositionschiffre,
der, formedelst dets utallige Afvexlinger, i Forening
med den største Simpelhed og Lethed, kan
gjøres aldeles uopløseligt, endog
for den, som har opfundet det
Ledsaget
af
en Forerindring, en Indledning og et Tillæg.
Med otte Kobbertavler og mange Tabeller.
- Ei blot til Lyst. -
af
I.B LINDENFELS,
Major af Artilleriet og Lærer ved de Kongelige Pager, ved Landcadetcorpset og Artillericadetinstitutet
Kjøbenhavn 1819
Trykt, paa Fr. Brummers Forlag, hos H.S. Popp.

Figure 45. Facsimile of the title page from *Den hemmelige Skrivekonst* (The Art of Secret Writing) published 1819. The motto: *Ei blot til Lyst* (Not only for pleasure) was reinscribed over the stage of the Royal Theatre in Copenhagen in 1817-18 after a heated public debate. At the rebuilding of the theatre in 1774, when it was originally introduced, Johan Herman Wessel, the witty satirical poet, remarked that it had truly been the joint contribution of all four directors. One had suggested *pleasure*, another *for*, a third *only*, whereupon the fourth had added a small *not*, because it looked better. In 1798-99, another poet, Jens Baggesen, used his prerogative as director to have it substituted by the Latin motto of the Opéra Comique in Paris: *Castigat ridendo mores* (It castigates manners through laughter). But this was resented by many who felt that the language should be Danish. Today, the inscription is taken for granted as part of the tradition of the theatre.

September 1939 at the age of fifty-nine. In fact, Mendelsohn did not even see the proofs of this article, which were corrected by his associate and friend, Lt. Col. William F. Friedman, then Principal Cryptanalyst in the Office of the Chief Signal Officer of the U. S. Army.

With this background in mind, we are hard put to find a more authoritative source on the history of the Vigenère cipher than the article by Mendelsohn. It is therefore noteworthy to read in Mendelsohn's abstract, that "*In all the literature of cipher, I know of only one writer who has correctly described Vigenère's cipher, and that was well over one hundred years ago*". In the body of the article Mendelsohn, referring to "*I. B. Lindenfels, Den hemmelige Skrivekonst (Copenhagen, 1819)*" [1]), expands on this remark by the assertion:

> "*Lindenfels, so far as I can ascertain, is the only writer who accurately presents both the table and the directions of Vigenère*".

On this authority, I have often relied on Lindenfels' work for factual information in past discussions. So far, I have withheld his story which, lying dormant in the Danish Army Archives and some contemporary bibliographical accounts, is perhaps as fascinating as the topic he describes. [16]) But first a few words about his book, to establish what its author has to say about himself and his intentions. Also, to put things in the right perspective, we shall briefly touch upon its contents and its role in Danish military history.

Its title page, shown in facsimile in figure 45, was engraved, so Lindenfels proudly tells us, together with nine other illustrations by a young artist, H. C. Klingsey, employed as a map-maker by the Danish navy. It reveals that Lindenfels was a major of the artillery and a teacher of the Royal Pageants (cadets training for general staff and military engineering), at the Land Cadet Academy (infantry and horse), and at the Artillery Cadet Institute. In the book, Lindenfels mentions that, "*on Royal Command*", he had written a French textbook and grammar. In other words, this contribution was officially appropriated as the teaching material in French, which agrees with the fact, documented in a protocol in the army archives, that his assigned "*science*" was "*French terminology*".

In the "prereminder", Lindenfels assures the reader that he has done everything in his power to make the book as entertaining as possible. Simultaneously, however, he emphasizes that his choice of the motto: "*Ei blot til Lyst*" (not only for pleasure) on the title page [17]), is made on purpose:

> "*All European have a larger or smaller collection of cryptographical works in their languages, whereas we in Denmark, as far as the author is aware, do not own a single letter hereof in the mother tongue. The author has therefore endeavoured, also in a*

scientific sense, not to be entirely unworthy in filling out this lacuna in the national literature. Both of these purposes unite in the 'pium desiderium' [pious wish]: *to enable our young officials – in particular the military – to match also in this respect those of our neighbouring nations. It is necessary in times such as ours, not to lag behind foreigners, especially in these things, if we do not wish at all hours to succumb to them".*

The explanation continuing under the subtitle of the book, refers to the fact that its dominating content is a "*new transposition cipher*". To the modern reader, this is outright misleading, for the cipher under discussion is neither new nor one of transposition. Indeed, as stated by Mendelsohn, it is the Vigenère cipher. By the terminological standard of today, Lindenfels is therefore dealing with a polyalphabetic substitution cipher. In those days, however, the terminology referred to the manner of data *representation*. If letters or numbers were used it was considered a transposition of the alphabet. Alternatively, when "*wholly marvellous signs*" were used, it was a substitution, if this word was applied at all.

The confusion arising from the word "*new*" is due to the fact that we think of invention, whereas Lindenfels referred to the introduction of a new practice to replace the simple substitution cipher or traditional nomenclature. Lindenfels was well aware of the venerable age of the Vigenère cipher, and he uses quite some space, in fact, to demonstrate that two ciphers, proposed by a Dr. Kluber of Tubingen in 1809, and by a Dr. Müller of Hamburg in 1818, are but reinventions of the contribution of "*old Vigenère*". Indeed, he emphasizes, about his own book, that,

"Thus, our 'Art of Secret Writing', is but a concentrated translation or quintessence of about one hundred published works, mostly referred to in this book by their complete title, and with the various quotations identified by page numbers"

Totaling close to three hundred pages, Lindenfels' "*translation*" is divided into three parts of about equal size: Simple substitution ciphers and nomenclatures; the Vigenère cipher; and a "*supplement*". The latter is not only a concentrated history of ciphers and codes, documenting some fascinating applications, but it goes beyond to the sign languages of thieves as well as of deaf and mutes. The first two parts are dated September, 1818, the latter 31 March 1819. The book was sold on subscription, so the reason for the delay in publication – and, hence, the expansion in size – Lindenfels gives as the difficulty of collecting the subscription list. The latter, which Lindenfels describes as unusual both with respect to the number of subscribers and to their high ranks and status in society, is reprinted in the front pages of the book. Thus, Frederik VI himself purchased ten copies, of which at least one is now in the Royal Library in Copenhagen.

Although somewhat archaic in its bombastic phraseology of the time, the book is evidently written by a man in perfect command of the Danish language, even

though towards the end, he hints at a fear of not having expressed himself well enough. Or, perhaps he realizes, as an afterthought, that his potential reader is not the perfect scholar and linguistic genius, he himself obviously is. None of his many quotations are translated into Danish, whether they are in Greek, Latin, German, or French. In fact, his two examples on how to break a simple substitution cipher, are in Latin and German, respectively!

Yet, when this is said, the book reflects upon its author the impression of a true Dane possessed, to quote Lindenfels himself, by "*the purest patriotism, the most fervent enthusiasm for the honour and welfare of King and country*". The surprising fact, however, is that Lindenfels was not at all Danish. He was an immigrant with Denmark as his adopted country. So, perhaps we may assume that he merely said it to survive. The facts of his life, as we shall now recount them, prove otherwise Lindenfels' assertion should be taken at face value.

Joseph Bennedict von Lindenfels was born in Vienna on 15 December 1762 and grew up partly in Paris, and partly in his native town. The data of his military career, according to the information he gave his commanding officer in the Danish Battalion, Royal Artillery Corps, on 29 September 1814, are recorded in the conduct or promotion list: "*Condutteliste for D'Hr. Officerer af det Kongelige Artillerie Corps danske Bataillon*", now in the Army Archives in Copenhagen. We can be pretty sure that every effort was made to make these data as correct as possible, for it was well known that Frederik VI studied these lists to get to know his officers. Indeed, what was not known at the time, was that the King went as far as to go through the subscription lists of military books such as Venturini's "*Lehrbuch der angewandten Taktik*" (textbook on applied tactics), published in Slesvig 1798, to see whether his officers did their homework. [18])

The facts pertinent for us, are that Lindenfels served in the Austrian Army, in Archduke Joseph's Dragoon Regiment from 1784 to 1792 when, at the rank of Captain of the Horse, he was granted the right to retire. It was during this period, from 1788-90, that he participated in the campaign against the Turks. The French Revolution had started in 1789, and so, like many intellectuals all over Europe, Lindenfels went to France enthusiastic about the new ideas. He offered his service to the Republican Government and, as an officer with war experience, he was promoted Lieutenant-Colonel and put in command of the First Battalion of the Mont Blanc Department in 1793.

The same year, Lyon rose against the French National Convent. A siege was therefore started against the unfortunate city, where Ampère, the famous physicist, in 1789 at the age of 14, witnessed the murder of his father, the mayor of Lyon, by a mob during the "Reign of Terror" following the Revolution. Lindenfels must have been among the highest-ranking officers in this siege, for his list of

publications contains the curious item: *"Aux Habitants de Lyon. Appel du Citoyen J. B. L. ,.. Lieut.-Col. et Comm. en Chef du prem. Bat. du Montbl. Lyon 1793"* (To the inhabitants of Lyon. Appeal by citizen J. B. L., etc.). The city did not surrender immediately. It was therefore destroyed by bombardment, and when it finally surrendered the National Convent started yet a reign of terror. Shocked by the cruelty and the killings he could not prevent, Lindenfels left France in 1794 after having been granted the right to retire. His high ideals about the French Revolution in ruins, he published his version of the siege in 1794-95, correcting, as an *"impartial eye-witness"*, a previous account by von Archenholz in the journal Minerva.

After a brief sojourn in Hamburg, he moved to Denmark early in 1796 together with his wife Caroline, née Egermann von Egerburg. Here they settled down in Odense, where nine years later Hans Christian Andersen was born. Amazingly, as it may seem, Lindenfels became part-owner and editor of the local newspaper. *Fyens Stifts Adressecomptoirs-Avis*. He must have picked up the Danish language fast, for by the end of the year, he took over the entire business and edited the newspaper single-handed until May 1798, when he sold it to become headmaster of *Det Schouboeske Institut*, recognized as the most advanced school in Copenhagen

The following years evidently fulfilled his desire for study and atonement. His home-life was no doubt happy and content, and from the army conduct list we know that his marriage was blessed with one child. It must also have been in this period that he acquired the knowledge later to be documented in his book on cryptography. In this work, he explicitly refers to the works of John Wallis, and, from his avowed interest in the problem of the handicapped, I cannot help feeling that Fourier's description of the latter also applies to Lindenfels: [9])

> *"The history of the sciences will recall that Wallis was one of the creators of an art precious to humanity, namely the education of the deafs and the mutes. By his efforts, many of the unfortunates succeeded to understand the English language, to write it, and even to pronounce it rather well. He was driven into this by a feeling of benevolence, which for him was quite natural, and he was guided by the philological studies of his youth".*

The happiness of this life and work lasted until the bombardment of Copenhagen by the British in 1807. The nightmare and the horrors of Lyon were once more a reality. A letter by the physicist Hans Christian Ørsted, rendered in figure 46, captures the situation. The reign of terror had come to Copenhagen. For the third time, Lindenfels took to arms. The vague ideals of his youth were gone. So were his illusions. But he now had a cause to defend, more tangible and earthbound, yet worthwhile fighting for. Peace and happiness. The three days in Copenhagen in 1807, form the sounding-board of Lindenfels' remark. He felt himself a Dane. His book on cryptography was the legacy to his adopted country.

Copenhagen, 8. September 1807

You must have seen in the newspaper that Copenhagen was besieged and has been bombed most horribly. I haste to bring you out of the anxiety for your friends which this might have caused you. We have endured 3 dreadful days and nights in which a large part of the city has been destroyed, for instance, the tower of Our Lady has burnt. At length we are out of danger; but 20 frigates and ships of the line are the prize for saving the city. Your father should have been the host of the English generals at Frederiksberg Slot, but has happily absolved himself from this function. Frederiksberg Have is not very much damaged, but the more so Søndermarken. My brother and your sister have not lost much, I almost nothing. On the other hand, state councillor Heger's estate has burned. I am not enough calmed down to write methodically, so you will have to accept rhapsodic news. Winkler is unharmed, Lehmann escaped death by a miracle but lost all he owned. The youngest three daughters of Professor Hornemann are wounded, and one of them will loose a foot. The number of those who are wounded, is exceedingly large. This manner of war is the most cruel of all, because in a period of 3 times 24 hours they showered the city with more than 12,000 bombs, incendiaries, etc., without any defense being possible. Add to this that they approached Denmark, acclaiming their friendship until the Islands were surrounded, 30,000 men ready to go ashore, and all arrangements of arsonite murder ready, then you have the picture of the state of affairs in Copenhagen.

When I can I will write you more. Give my regards to Koes and Brøndsted.

Yours,
H. C. Ørsted

[PS.] I learned at the post office, attempting to mail the above letter, that they did not accept letters going out of the country. Today, finally, the mail goes to Hamburg but, as I hear just now, much earlier than usual. I will therefore have to rush. Almost a week has passed since the capitulation. All is quiet but the sailors are furious. Our navy is now being rigged by the English in all haste. Within a month perhaps we may find ourselves completely free from them, and will only then be able again to enjoy the peace so dearly bought. Rest assured that every Danish citizen would gladly have dared and sacrificed life and blood to save Denmark's Pearl, if one could not have calculated the impossibility of stopping the destruction of the city from which anyhow the loss of the navy would have followed. Whether the rulers could have prevented the city from coming to this point, I dare not say.

The Englishmen are behaving very courteously, so that one can see that among them manners exceed nature. Only the accompanying Highlanders do not submit to any discipline

Figure 46. Letter about the bombardment of Copenhagen by the British in 1807, from the physicist Hans Christian Ørsted to the poet Adam Oehlenschläger, then studying in Germany. Ørsted's brother had married Oehlenschläger's sister. Oehlenschläger's father was the Royal Keeper of the palace Frederiksberg Slot and its surrounding parks Frederiksberg Have and Søndermarken. The British used the tower of Our Lady's church to aim their guns and incendiary rockets, the latter being here introduced as a new weapon of terror.

About Lindenfels himself, there is not much more to tell. He was the industrious author of a series of smaller contributions on various subjects, so perhaps we might say that he once more took up his journalistic career. Granted permission to retire in 1821, he moved to Altona, now a suburb of Hamburg, but then on the Danish border. There he died on 16 February 1833 at the age of seventy-one.

There is one question, however, that we need to raise; namely, whether his book was ever adapted as a textbook or at least influenced the teaching of cryptography at the military academy. Unfortunately, this question must remain unanswered. Undoubtedly, ciphers and their use have been mentioned in the teaching, but it has not been possible to document the existence of a proper course. In fact, the army archives contain no indication that cryptography was used in the Danish army prior to the introduction of the cryptographical devices by Count Orloff in 1873 and by Captain Sommerfeldt in 1883, which I mentioned in connection with the discussion of Julius Petersen's cipher (see section 2.7). [18])

As to the more sporadic discussions, Lindenfels gives two examples in his book which throw an interesting sidelight on Ørsted's many-sided activities, and therefore deserve to be mentioned

One incidence relating to Ørsted's background as a pharmacist, has to do with the disclosure of invisible, so-called sympathetic ink. Here, Lindenfels recommends five tests, remarking in a parenthesis about his first two, namely "*holding the paper up against the light, warming or heating it over live coals;*" that:

> "*... according to Professor Ørsted's assertation, these two tests will enable one to discover, almost without exception, all kinds of concealed, or with sympathetic ink composed, writings*".

The other example is perhaps the most interesting, because it infers how Ørsted gradually worked towards his discovery of electromagnetism in 1820, about a year after Lindenfels had put his account on print. In the main text, Lindenfels offers the following bombastic remark, which undoubtedly was inspired by Ørsted's lecturing and demonstrations:

> "*Who, by the way, does not know the wonders which are caused by the newest galvanic and electric discoveries and, on the whole, by the daily increasing and to the incredible bordering progress in physics and chemistry? Who does not know that, among other things, one can now correspond in a simple manner, aided by these almost recreated sciences,* beneath or through the earth *and thus, in times of war, or under blocade or siege, can entertain a mutual* secret *communication between important cities and garrisons, such as Copenhagen and Kronborg* [Elsinore Castle]".

Looking back at this rhetorical statement, Lindenfels evidently became aware that he was one of the privileged few who had heard Ørsted and others expound

on the latest scientific discoveries. He therefore felt called upon to give the following explanation in a footnote.

> "*A highly surprising specimen of such a novel cypher or secret manner of writing (invented by State Councillor Sommering, the famous anatomist, member of the München Academy, etc.) was demonstrated in January, 1817, at the Royal Military Academy, by our meritorious professor, Knight Ørsted, at a public examination attended by His Majesty the King. This specimen was examined very attentively by the Monarch himself, and received deservingly the Royal admiration and highly honourable acclamation*".

3.3 The Vigenère Cipher

Of the various names given the cipher of our story, perhaps the most appropriate is the "*chiffre carré*", the tabular cipher. Becoming popular during the French Revolution, it was called by Dlandol, in his book: *Le contr'espion, ou les clefs de toutes les correspondances secrètes* from 1794, the "*chiffre par excellence*". During the Napoleonic wars, acquiring a reputation of extreme safety, it came into widespread use as the "*chiffre indéchiffrable*". This appellation, and the associated preeminence, the cipher enjoyed for more than a century. Today, as mentioned earlier, it is usually known as the *Vigenère cipher*, after the French diplomat and scholar Blaise de Vigenère, Bourbonnais, who in 1586 described it in his classic treatise: *Traité des chiffres ou secrètes manières d'escrire.* [19])

Among the endless number of ciphers discussed in this compendium of sixteenth-century knowledge of cryptography, the cipher now given Vigenère's name, is not the most relevant choice. In fact, Vigenère made only one claim on this cipher, scrupulously assigning all credit to earlier writers such as Abbot Trithemius (Johannes Trittenheim), Giovanni Battista Belaso (or Bellaso), and Giovanni Battista Porta. Yet, by a curious twist of fate, he was robbed by posterity of his single contribution to this cipher, the so-called *autokey*, which turned up again in the nineteenth century as an invention of the day

Although so common in use that it has been dealt with by almost every writer on cryptography since Vigenère, it has been reinvented time after time; and always with exaggerated claims of its invulnerability by the headstrong amateur inventors. Truly, as late as January 27, 1917, it appeared under the heading: *A New Cipher Code* in the reputed journal, Scientific American, which claimed: [20])

> "*The publication of this cipher code will no doubt bring to the mind of the reader other codes, but it is doubted if any heretofore invented is as effective in every way as is this one*".

On its way to glory, the Vigenère cipher was broken only occasionally, and mostly by a lucky guess. Porta, characterized in our time as the outstanding cryptographer of the Renaissance, gave a few illustrations in his book: *De Furtivis Literarum Notis*, printed in 1563. For example, challenged by an amateur he correctly surmised that the key was a common proverb. Moreover, in the second edition from 1602, he took a first step towards a consistent analysis based on his discovery that a multiply repeated letter in a cryptogram signals the joining of alphabetic sequences of letters in the plaintext and the key, with one of these sequences in reversed order. Advancing certain simplifying premises, John Falconer, a distant relative of the Scottish philosopher David Hume, even provided an expedient cut-and-try method in his book: *Cryptomenysis Patefacta*, published posthumously in 1685. Thus, assuming a normal cipher alphabet and preservation of the original word divisions, he explained how, by guessing the short words, it is possible to gradually deduce the letters of the repeated key. [21])

Still, what finally brought down the Vigenère cipher after almost 300 years of vain efforts, was the analytical technique for determination of the key periodicity proposed in 1863 by a retired infantry major in the Prussian army, Friedrich W. Kasiski. [22]) The shrewd observation on which this technique capitalizes, is that the conjunction of a repeated part of the key with a repetition in the plaintext will produce a repetition in the cipher text. Kasiski devoted a major part of his 95-pages short volume: *Die Geheimschriften und die Dechiffrierkunst* to this epochal discovery, but the book stirred no interest at the time. Kasiski therefore abandoned cryptography and turned to the subject area of anthropology, joining the Natural Science Society of Dantzig, unearthing prehistoric graves, and reporting his work to learned journals. [12]) He died in 1881.

By more than a decade, however, Kasiski was preceded by another cryptographer con amore, who broke the secret of the Vigenère cipher. This man was Charles Babbage. In fact, Babbage went further than Kasiski, for he established the law of the cipher.

In a footnote to his discussion of Friedman's index of coincidence, Kullback remarked: [13])

> *"Indeed, we might venture to define cryptanalysis as the solution of cryptograms by an analysis and application of the 'invariant' characteristics of the cryptographic system employed. A cryptographic system which has no invariant characteristics would be secure against unauthorized decipherment".*

Applying mathematical reasoning, Babbage succeeded in describing the invariant properties of the Vigenère cipher in the form of a law. This turned a craft into a science. To follow in his footsteps, we shall therefore complement our conventional presentation of the Vigenère cipher by a mathematical interpretation.

A prerequisite to the use of the Vigenere cipher, is a so-called *tableau*. Figure 47 shows Lindenfels' reproduction of Vigenère's original tableau from 1586. *"Such tableaux"*, says Lindenfels, *"look almost like a multiplication table and, for the encipherment and the decipherment, they are used in the same way as such a one"*. Thus, if the "multiplicator" is sough in the left column of non-italic capitals, and the "multiplicand" in the upper row of non-italic capitals, then the "product" is the lower-case letter specified in the body of the table by the intersection of the two factors. Accordingly, if we let the key, say the name *"Cain"*, correspond to the "multiplicator", and the dispatch, say the name *"Abel"*, to the "multiplicand", then, pairing the letters one to one, we find that the "product" or cryptogram is the word *"uhis"*. Alternatively, if the italic capitals are used to denote the "factors", then the "product" or cryptogram will be the word *"qpeo"*.

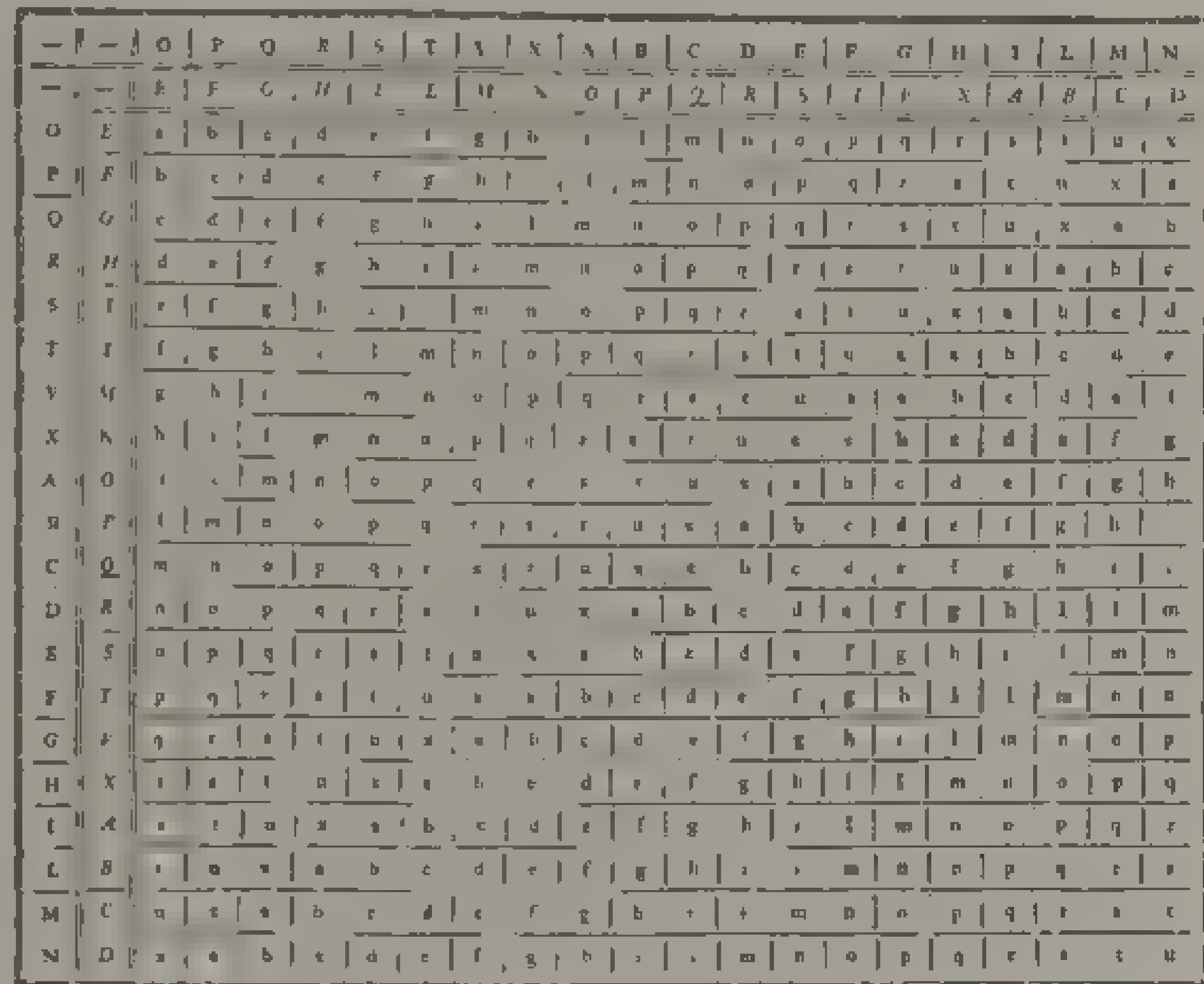


Figure 47. Lindenfels' reproduction in 1819 of Vigenère's tableau, as given by the latter in his *Traicté des Chiffres*, Paris 1586.

```
* * * VIGENERE CIPHER * * *

TO ILLUSTRATE THE USE OF A VIGENERE TABLEAU T, LET
IT BE BASED ON THE FOUR-LETTER ALPHABET   L← EABC

BY VISUAL INSPECTION

ENCIPHERMENT                          DECIPHERMENT
KEY K           B A B E               KEY K           B A B E
PLAINTEXT P     A B B A               CIPHER C        C C E A

CIPHER C        C                     PLAINTEXT P     A

FOR INDEX I=1  C[1]←C                 FOR INDEX I=1  P[1]←A
FROM  K[1]=B & P[1]=A                 FROM  K[1]=B & C[1]=C
TRACING THE TABLEAU                   TRACING THE TABLEAU

K[1]=B                                K[1]=B

              | E A B C |                           E A B C
P[1]=A   →→→A→B→C E |                 C[1]=C        A←B←C E
              | B C E A |                           B C E A
              | C E A B |                           C E A B

BY APL INDEXING

ENCIPHERMENT                          DECIPHERMENT
SINCE ALPHABET L EQUALS               SINCE ALPHABET L EQUALS
THE FIRST ROW T[1;]                   THE FIRST COLUMN T[;1]
LET US INTRODUCE                      LET US INTRODUCE

1                                     1
FOR ALL INDEX I, SAY                  FOR ALL INDEX I, SAY
  I←1                                   I←1
WE PROCEED COLUMNWISE                 WE PROCEED COLUMNWISE

3                                     3
                                        T[L⍳K[1];]
                                      BCEA
AND ROWWISE                           AND ROWWISE

                                      2
OBTAINING THE RESULT                  OBTAINING THE RESULT

                                      A

ENCIPHERING IN GENERAL

CEA
```

 Figure 48. How to use the Vigenère cipher.

```
* * * BEAUFORT CIPHERS * * *

A BEAUFORT TABLEAU IS MERELY A VIGENERE TABLEAU T
WITH ITS FIRST ROW AND COLUMN REPEATED AS ITS LAST
ROW AND COLUMN, RESPECTIVELY.  NEGLECTING THIS, WE
SHALL EXPLAIN ITS USE ON THE ALPHABET   L←'EABC

TRUE CIPHER

ENCIPHERMENT                          DECIPHERMENT
KEY K           B A B E               KEY K           B A B E
PLAINTEXT P     A B B A               CIPHER C        A C E C

CIPHER C        A                     PLAINTEXT P     A

K[1]=B                                K[1]

              | E A B C |                           | E A B C |
P[1]=A   →→→A→B C E |                 C[1]=A   →→→A→B C E |
              | B C E A |                           | B C E A |
              | C E A B |                           | C E A B |

OR, BY APL INDEXING                   OR, BY APL INDEXING

A                                     A

VARIANT CIPHER

ENCIPHERMENT                          DECIPHERMENT
KEY K           B A B E               KEY K           B A B E
PLAINTEXT P     A B B A               CIPHER C        C A E A

CIPHER C        C                     PLAINTEXT P     A

K[1]=B                                K[1]=B

              | E A B C |                           | E A B C |
              | A B C E |                           | A B C E |
              | B C E A |                           | B C E A |
P[1]=A        | C←E←A B |             C[1]=C   →→→C→E→A B |

OR, BY APL INDEXING                   OR, BY APL INDEXING
  L[T[L⍳K[1];]⍳P[1]]                    T[L⍳C[1];L⍳K[1]]
C                                     A
```

Figure 49. How to use Beaufort's cipher and its variant.

Clearly, the capital letters, exemplified here in non-italics and italics, serve as indices to the tableau. That is, we are to use the tableau, to quote Vigenère himself,

> " *taking the capitals which run across the top for the message to be conveyed and those that run perpendicular downward at the left for the keys. I have put two rows of capitals here, one black* [non-italic], *the other red* [italic], *to show that the alphabets of the text as well as of the keys may be transposed and changed at will to keep knowledge of them from all except one's correspondents*".

As any cryptographer will admit, the permutation of the "capital" or index alphabets, is a complication which makes it far more labourious to break the cipher. Also, in the illustrative examples it tends to obscure the basic patterns. In the following, therefore, we shall assume that the first (left) column and the first (top) row of the body of the table will serve as the defining sets of alphabetic indices. Further, we shall find it convenient to introduce the opposite standard of Vigenère, in that we associate the key with the first or upper row. Of course, since the tableau is symmetrical about its main diagonal, this change of standard will not affect the outcome.

With this proviso, let us now take a closer look at the encipherment and decipherment processes for a Vigenère cipher. This is done in figure 48 for a scaled-down version based on a four-letter alphabet. It is readily appreciated by comparison with figure 47, that the four-by-four tableau of our model is similar to the body of lower-case letters in Vigenère's original tableau. In particular, we see that both tableaux exhibit the characteristic diagonal pattern, containing the same letter in any given diagonal from lower left to upper right.

A life-long friend of Babbage's and supporter of his work on the Difference and Analytical Engines, was Rear-Admiral Sir Francis Beaufort, R. N. [3]) Thus, in Babbage's fight to reform the Royal Society to end, what he considered, its neglect of science, Beaufort, then a captain, repeatedly sided with Babbage even to the point of declining to sit on the Council. Similarly, he warmly recommended Lord John Russell, then prime minister, that the government continue its economic support of Babbage's work on his computers. Beaufort's best known scientific contribution was the so-called Beaufort scale, grading wind velocities on an ordinal scale from 0 (calm) to 12 (hurricane). This scale, it may be recalled, was in use until a few years ago, when it was substituted by measurement of wind velocities in meters per second.

Whether Beaufort and Babbage ever happened to discuss ciphers, is not known, but a few months after Beaufort's death in 1857, his brother published his invention of a new system of secret writing "*adapted for telegrams and postcards*". Actually, the system was a reinvention of a forgotten one, published in Rome in


```
IN GENERAL, THE INTEGRAL POWERS N OF A PERMUTATION
P ARE FOUND BY INDEXING, BASED ON THE DEFINITIONS
    (P*N)←→P[P...[P[E]]...]]  UP TO N FACTORS
         E←⍳⍴P   P*0←→E   &   P*(-N)←→⍋P*N
WHICH MAY BE IMPLEMENTED BY A RECURSIVE FUNCTION

               ∇ FOLD[⎕] ∇
             ∇ R←P FOLD N
         [1]   →((N>0),N=0)/CONTINUE,END
         [2]  NEGATIVE:N←|N
         [3]   P←⍋P
         [4]  CONTINUE:R←P[P FOLD N-1]
         [5]   →0
         [6]  END:R←⍳⍴P
             ∇

TO ILLUSTRATE, CONSIDER POWERS OF    P←2 3 4 1
     P FOLD ¯3          P FOLD 0          P FOLD 3
 2 3 4 1           1 2 3 4           4 1 2 3
```

Figure 50 Integral powers of a permutation

1710 by one Giovanni Sestri, although today it is known as the *Beaufort cipher*. [12]) The system, which is related to the Vigenère, also gave rise to a variant. Since both systems will be of interest to us, their use is explained in figure 49.

In principle, all three cipher systems: Vigenère, Beaufort, and the variant, are based on the Vigenère tableau. It will therefore be of importance to consider this tableau from a mathematical point of view.

Earlier, we quoted Lindenfels for the remark, twice repeated in his book, that the tableau resembled a multiplication table. Undoubtedly, the reader has already noticed that our tableau for the four-letter alphabet, is in fact the multiplication table from our automobile example. We shall now give this multiplication table a new interpretation. A prerequisite here, is an extension of the idea of the integral power of a number to that of a permutation. This little problem is dealt with in figure 50, which also provides an APL-function for its implementation: With this concept established, we are now ready to pose the question: What is a Vigenère tableau? The answer, which is given in figure 51, is that it is the multiplication table of a cyclic group.

To appreciate the deeper significance of this statement, it may be worthwhile to consult the use of the APL-function *SHIFT* in the APL Terminal Session of part 1 (see page 56). The purpose of this function was to produce the generatrices of an arbitrary string of text by "*running it down the alphabet*". We now see that the mathe-

matical interpretation of this process, is that it is composed of two things: the establishment of the carrier for a group of cyclic shift operations (APL's primitive *rotation*), and the application of this carrier to a single operand, the alphabet.

Thus, the abstract or neutral formulation of the multiplication table of a cyclic group, permits us to visualize how one and the same algebraic structure may be given different interpretations (or representations). On one hand, the multiplication table is identified as a Vigenère tableau. On the other, it is considered the operation on some text, running it down the alphabet. In either case, we realize that a complete description is given by identification of the group generator, namely the rotation or cyclic shift, and the operand, being here the alphabet. The way cryptographers explore this invariance or algebraic structure, is that they establish and investigate the carrier of the group forgetting all about the multiplication table. This is the inherent weakness of invariance referred to by Kullback. This, as we shall now see, is the "*law of a cipher*" discovered by Babbage

3.4 How to Impale a Law

Babbage had an only and beloved younger sister, Mary Anne, with whom he remained on warm terms for life. Revealing of his attitude towards her, is the fact that when she married Henry Hollier, he persuaded his closest friend, John Herschel, to become one of the trustees of her marriage trust. In close touch, the Holliers were frequent guests at Babbage's home in Dorset Street. Later, from about 1850 when they had moved to Lynmouth following Henry Hollier's retirement, Mary Anne and her children used to stay with Babbage, whenever they were in London

To entertain the children, Babbage initiated them into cryptography. Undoubtedly, he thereby recruited some dedicated and enthusiastic assistants, helping him with his code-breaking dictionaries. Also, he aroused an interest which they sustained into adulthood.

In February, 1846, one of these youngsters, his nephew Henry Hollier, Jr., challenged Babbage to solve a Vigenère cipher based on a conventional alphabet. Divided into three parts, each with a separate key, the cryptogram itself is not particularly interesting. In truth, the application is standard, and the message trivial. Yet, Babbage's solution makes it one of the most intriguing problems in the history of secret writing. It demonstrates how, by the introduction of mathematics, a law is discovered. It is the story about this solution that we shall now unravel from Babbage's worksheets. [23])

The covering letter enclosed with Henry's cipher, is transcribed in figure 52. Babbage has scrawled "*21 Feb. 1846*" on its top. That, however, is manifestly wrong,


```
                 * * * VIGENERE TABLEAU * * *

    THE VIGENERE TABLEAU IS A SQUARE TABLE THE ROWS OF
    WHICH FORM THE SEQUENCE OF ALL CYCLIC SHIFTS OF THE
    THE FIRST ROW, THE SO-CALLED  ALPHABET , ASSUMED TO
    CONSIST OF NON REPEATED CHARACTERS OR INTEGERS

    TABLEAU T ON A FOUR-LETTER ALPHABET, L←'EABC', IS

                   +     + +      + +      +
       LEFT OR     | 0⌽L | | EABC | |  0⌽L |  RIGHT OR
    ANTICLOCKWISE  | 1⌽L | | ABCE | | ¯3⌽L | CLOCKWISE
      ROTATION     | 2⌽L |←→| BCEA |←→| ¯2⌽L | ROTATION
        N⌽L        | 3⌽L | | CEAB | | ¯1⌽L |   (-N)⌽L
                   +     + +      + +      +

    BASED ON THE IDENTITY   N⌽L←→(N-⍴L)⌽L

    THE ANTICLOCKWISE (OR CLOCKWISE) ROTATIONS
     0⌽L   1⌽L   ...   N⌽L    WITH  N= 1+⍴   &  L=0⌽L
    WHEN PERFORMED IN SUCCESSION, FORM A GROUP WITH THE
    TABLEAU AS MULTIPLICATION TABLE. TO ILLUSTRATE, PUT
       []←E←L        []←A←1⌽       []←B←2⌽L        []←C←3⌽L
    EABC          ABCE              BCEA             CEAB
    AND THE SIMILARITY, THE SO-CALLED ISOMORPHISM, IS
    VERIFIED BY COMPARING THE MULTIPLICATION TABLES

              +                  +    +----------+
              | L   1⌽L 2⌽L 3⌽L  |    | E A B C  |
                1⌽L 2⌽L 3⌽L L    |      A B C E
              | 2⌽L 3⌽L L   1⌽L  | ←→ | B C E A
                3⌽L L   1⌽L 2⌽L  |      C E A B |
              +                  +    +----------+

    BECAUSE OF THIS INTERPRETATION THE GROUP IS KNOWN
    AS THE CYCLIC GROUP OF ORDER 4, DENOTED  C4  SINCE
    THERE IS ONLY ONE CYCLIC GROUP OF EACH ORDER, OR
    NUMBER OF ELEMENTS, THE VIGENERE TABLEAU DEFINES
    A CYCLIC GROUP  CN, OF ORDER  N=⍴L

    THE DEFINING CHARACTERISTIC OF A CYCLIC GROUP, IS
    THAT IT IS GENERATED BY A SINGLE GENERATOR   1⌽L,
    OR ITS INVERSE  (¯1+⍴L)⌽L, BY TAKING ITS  POWERS
    FOR EXAMPLE, SINCE  A←1⌽L  IS THE GENERATOR OF THE
    CYCLIC GROUP C4, WE CAN DEFINE ITS INTEGRAL POWERS
     A*N←→N⌽   A*(-N)←→N⌽(1+⍴L)⌽L  &  A*0←→E WITH E←L
    THIS GIVES RISE TO YET A GROUP REPRESENTATION

                    +----           --  +
                      E   A   A*2 A*3   |
                      A   A*2 A*3 E     |
                      A*2 A*3 E   A     |
                      A*3 E   A   A*2   |
                    +-                  +
```

Figure 51. What is a Vigenère tableau?

Richmond Park, Feb. 1846
My dear uncle,

I enclose a note from me to you *which it will afford me much pleasure to find that Mr Lefevre or Mr. Babbage or any other man of the most acute intellect or unwearying perseverance can decypher: whenever your friends are* satisfied *they are beat I shall be able to show them how very easy it is to decypher when the principle is* explained *& that the principle though of the* simplest *in the world when* known, *is also the most puzzling when unexplained – –*

Believe me
Ever your affectionate nephew
Henry

PS. You will observe that to prevent the lyu in the 7th [5th] *line from being mistaken for Gin I have put a pencil mark at top to explain it is l y i u.*

Wishing your philosophic friends
joy of their little talk – again
Yrs Affy Henry

Figure 52 Note accompanying Henry's challenge
(BL, Add Ms. 37205 F. 48)

for there are worksheets dated prior to that date. The earliest I have found, is marked "*Wednesday, 18 February 1846*", (folio 44-1). All Babbage's notes, even the earliest, seem implicitly to assume that the cipher is a Vigenère based on a standard alphabet. Presumably, this was an educated guess derived from a letter frequency count. Let me also add, that in his indexing, as I have remarked before, Babbage relied upon the use of a 1-origin

Figures 53 A & B summarize the contents of his worksheets. They begin with a statement of Henry's cipher, such as Babbage copied it, describing its solution to his lifelong friend, Edward Adolphus, the Duke of Somerset (folio 63). One of the most influential supporters of Babbage's Difference Engine, the Duke was an avid geometer who published, as we know from Babbage's library, at least two works on the geometrical relationship between circles and ellipses. His name will turn up shortly since Henry used it as a keyword; but let me not anticipate things

After some preliminary probings, for example listing 2- and 3-letter words, the first important worksheet, dated "*20 Feb.*", carries the note: "*Try to find the key to each letter by affectionate*", (folio 44-2). Observing that the plaintext letter "*E*" is twice enciphered as "*I*", Babbage makes his initial attempt (see figure 53 A) to extend the notion of linear equations to congruences. How he got on to the idea here, is in the dark. Although it is evident that he often attempted to reap the practical benefits of Gauss' mathematical contribution to this topic area. In his *Passages*, for example,

he described how the concept of principal remainders might be used to decide a conditional statement for his proposed automaton, playing the game of "tic-tac-toe", whenever the different moves were "*equally conducive to his winning the game*". Thus, letting "*the machine keep a record of the number of games it had won from the commencement of its existence*", he simply divided that number by the number of options at hand, directing the machine to take the course determined by the resulting principal remainder. To this explanation he added philosophically:

> "*It is obvious that any number of conditions might be thus provided for. An inquiring spectator, who observed the games played by the automaton, might watch a long time before he discovered the principle upon which it acted. It is also worthy of remark how admirably this illustrated the best definitions of chance by the philosopher and the poet: –*"

"Chance is but the expression of man's ignorance." – Laplace
"All chance, design ill understood." – Pope

But let me get back to the cryptographical problem. Evidently, Babbage's aim was to come up with an independent set of simultaneous equations, one for each suggested plaintext letter, so that their combined solution would uniquely determine the key letters. However, his set of equations was incomplete. The number of unknowns exceeded that of independent equations, so as to admit an infinity of solutions.

He therefore revised his approach (see figure 53 A), introducing a kind of vectorial approach, which in his manuscripts is signaled by the note: "*Take 26 from all the +s* [i.e. sums] *exceeding 26*" (folio 57). Evidently, he here assumed an alphabet of 26 letters. On a worksheet dated "*Twentyfourth of February*", this approach provided the break-through, and he found the key: "*Somerset*". But even more important, it led him to the significant observation that the alphabet was shifted cyclically one position. However, since the key failed to translate the introduction of the letter, he guessed a new plaintext fraction: "*Dear Uncle*", and used it to repeat the process. By virtue of the fact that the letter "*U*" was enciphered into itself, he ran into a boundary case (see figure 53 B). This he solved by introducing a new rule, saying that index zero should be substituted by index 26. Thus, he arrived at the second keyword "*Murray*", which name he explained in a brief note, jotted down on the top of one of his sheets (folio 47): "*Murray is Mr. Grove, 16 Chesham Place*".

Applying these two keys to the rest of Henry's cryptogram, Babbage soon convinced himself that neither of them, not even reversed or run down the alphabet, could have been used to encipher its main body: Lines 2 to 6 (incl.). The remainder of his notes, therefore, are devoted to calculations in search for yet a keyword. Undoubtedly, since the other two keys were names, Babbage assumed the

```
        PYRI ULOFV
             POVVMGN MK UD GOWR HW LQ PGFJNYQ
        OJAV MSN WIJHEEHPR BRVGRUHEGK. EFF WJSR RVY
        CPOY VSP. PX OKLN PI XXYSNLA SELF XG
        FEEWTALV LJIU, VR NOI EGAP HMFL ML YINZ
        TNGDDG YGIV UYEAP BQL
                  WJQV POYK STRITLMHFOFI
                            EWTAWK
                                      TIEJC

PROBABLE WORD    A F F E C T I O N A T E    WITH    E E
                 S T R I T L M H F O F I            I I

INITIAL ATTEMPT

LET VECTOR  X  WITH  (12=⍴X)  DENOTE THE ASSOCIATED KEY
FRACTION AND  A, B,  &  C  THREE UNKNOWN CONSTANTS. THEN
WITH ALPHABET  ABC  WE HAVE THE ARITHMETIC CONGRUENCES
   (ABC⍳'E') = (⍴ABC)|(A×ABC⍳'I') + (B×ABC⍳X[4]) + C
   (ABC⍳'E') = (⍴ABC)|(A×ABC⍳'I') + (B×ABC⍳X[12]) + C
FROM WHICH WE DERIVE
    (B×ABC⍳X[4]) = B×ABC⍳X[12]      OR      X[4] = X[12]

CONSIDER THE TRANSLATION OF THE PAIR OF DOUBLE PLAINTEXT
LETTERS   FF,  INTO THE PAIR OF DIFFERENT CIPHER LETTERS
TR   THE CONGRUENCES OF WHICH
   (ABC⍳'F') = (⍴ABC)|(A×ABC⍳'T') + (B×ABC⍳X[2]) + C
   (ABC⍳'F') = (⍴ABC)|(A×ABC⍳'R') + (B×ABC⍳X[3]) + C
GIVE THE NEW CONDITION
   ((ABC⍳'R') - ABC⍳'T') = ((ABC⍳X[2]) - ABC⍳X[3])×B÷A
WHERE THE LEFT HAND SIDE EVALUATES
           (ABC⍳'R') - ABC⍳'T' ↔ 17 - 19 ↔ ¯2

CLEARLY, EVERY NEW SUCH CONGRUENCE CARRIES WITH IT A NEW
AND UNKNOWN KEY LETTER.  HENCE, IT IS IMPOSSIBLE TO FIND
THE THREE UNKNOWN CONSTANTS   A, B,  &  C

[illegible]

NEGLECTING THE THREE CONSTANTS, LET US NOW INSTEAD FOCUS
ON THE CONGRUENCE OF THE DIFFERENCE.

P←ABC⍳'AFFECTIONATE'↔ 1  6  6  5  3 20  9 15 14  1 20  5
C←ABC⍳'STRITLMHFOFI'↔19 20 18  9 20 12 13  8  6 15  6  9

      (⍴ABC)|C - P    ↔18 14 12  4 17 18  4 19 18 14 12  4

HERE, BABBAGE DISCOVERED THAT IN A SHIFTED ALPHABET
           1⌽ABC ↔ BCDEFGHIJKLMNOPQRSTUVWXYZA
THIS DIFFERENCE REPRESENTED THE NAME
   X ← (1⌽ABC)[(⍴ABC)|C-P] ↔ S O M E R S E T S O M E
WHICH REVEALED THE KEYWORD.

THIS EXPLAINS BABBAGE'S OBSERVATION OF THE REPEATED KEY
LETTER   'EE' = X[4 12],  AS DUE TO A KEY REPETITION
```

 Figure 53 A. Henry's cipher.

```
YET A KEY WORD

HOWEVER, BABBAGE FOUND THAT THE KEY  SOMERSET  FAILED TO
TRANSLATE BUT THE LAST THREE LINES   7, 8, & 9.  HENCE,
HE HAD TO GUESS A NEW WORD.

    PROBABLE WORD   D E A R U N C L E        WITH    U
                    P Y R I U L O F V                J

BOUNDARY CASE

CONSIDER THE CONGRUENCE OF THE DIFFERENCE

    P←ABC⍳'DEARUNCLE'  ↔  4  5  1 18 21 14  3 12  5
    C←ABC⍳'PYRIULOFV'  ↔ 16 25 18  9 21 12 15  6 22
    ------------------------------------------------
     X ← (⍴ABC)|C-P    ↔ 12 20 17 17  0 24 12 20 17

HERE, A ZERO VALUED INDEX OBTAINS IN THE FIFTH POSITION
BECAUSE OF THE COINCIDENCE OF LETTER 'U'   SINCE THIS IS
WITHOUT MEANING IN A 1 ORIGIN, BABBAGE SUBSTITUTED IT BY
THE VALUE   26 = ⍴ABC,  CORRESPONDING TO THE POSITION OF
OF LETTER 'A'  IN THE ROTATED ALPHABET   1⌽ABC.  THUS,

 WITH X[5]←26  WE FIND  (1⌽ABC)[X] ↔ M U R R A Y M U R

SEARCHING FOR A THIRD KEY

TO TRY A  GUESS  (PROBABLE WORD OR KEY) ON A CRYPTOGRAM,
 CRPT , WE MAY NEED TO SLIDE IT OVER ALL POSITIONS.  A
CONVENIENT FUNCTION WHICH ALIGNS THE RESULT ROWWISE, IS

    ∇ R←CRPT TRY GUESS ⎕IO
[1]  ORIGIN ⎕IO←0
[2]  [illegible]
    ∇

TO ILLUSTRATE, ASSUME THAT WE BELIEVE THAT THE FRACTION
               AUX← ALVLJIJVRMDI'
CONTAINS THE WORD  'THE'. THEN, INVOKING  TRY , WE FIND
THAT THE KEY FRAGMENT IS EITHER 'THE' (AGAIN) OR 'HER':
               AUX TRY 'THE'              AUX TRY 'HER'
      HER                        THE
      SOM                        FRU
      CEF                        DMS
      SCE                        EFR
      QBQ                        CED
      PNR                        BQE
      BON                        NRA
      CKI                        ONV
      YFK                        KIX
      THE                        FKR
      VBW                        HEJ
      PTH                        BWU
IN FACT, THE CORRECT THIRD KEY IS THE NAME  'CACOETHES'.
```

Figure 53 B. Henry's cipher.

third one to be a name too. Thus, he adopted a kind of iterative technique, guessing interchangeably on probable keys and probable plaintext words.

To illustrate, by way of keys he considered a host of seven-letter names: EDWARDA, ADOLPHU, [i.e. Edward Adolphus, Duke of Somerset]; DANMORE, EARLOFD, etc., all matching the first word of the cryptogram: "*POVVMGN*". He then switched to DEARUNC, UNCLEUN, and back again to the name GLANVILLE

Still unsuccesful, Babbage tried his hand at probable plaintext words, focusing on the word: "*UYEAP-BQL*" which, presumably using the lost dictionaries, he gave an incredible list of interpretations from BIRTH-DAY to WOOLS-CAP. Yet, without luck. The for us today amusing fact, not discovered by Babbage, is that by this word Henry referred to Babbage's "*brain-box*", in that he concluded his message to Babbage with the pious hope that the cipher would: "*puzzle your brain-box*".

Leaving the realm of inspired guesses, Babbage now turned to the more tedious job of investigating the short words of 2, 3, and 4 letters. For example, he correctly guessed that the word: "*MOI*" interpreted as "*THE*", produced "*THE*" again as a fraction of the key. For a while this led him off the track, making him think that Henry had used the plaintext itself as a key, a so-called *autokey*. Thus, he wrote (folio 54): "*Since the word MOI has its key the same as itself it may be worth trying other words, but this is perhaps accidental and can only apply to odd letters in the cypher*".

In a search based on a list of normally *frequent trigrams:* THE, AND, THA, ENT, ION, TIO, etc., such as that of Babbage's, it is necessary to try these guesses against any possible fragment of the same length in the cryptogram. Following in Babbage's footsteps in the search for a third key (see figure 53 B), this is done by invoking an appropriate APL-function called *TRY*. Thus, sliding the plaintext word "*the*" across the fraction of the cryptogram assigned to the variable *ALX*, we find that a potential fraction of the key could be either "*HER*", "*SCF*", "*BON*", or

My dear uncle,

I feel quite annoyed that your scientific friend should employ his valuable time in seeking to discover what is past finding out, *as I can easily satisfy him whenever he gives up his* fruitless *exertions, for fruitless they* must ever be.

Pray, let me know as soon as he gives up the prosecution of the task and I shall have much pleasure in explaining it to both you and him

Ever your affectionate
Nephew Henry

March 19, 1846

Figure 54. Henry's second note
(BL, Add Ms. 37205 F 62)

"*THE*". In practice, each of these trigrams must now be tried against the text, using the same APL-function, to see if they should produce any plaintext at regular intervals (revealing the key repetition). In the figure, only the first of these potential key fractions is tested, and with a negative result.

Anyhow, Babbage did not go that far. Back again on the assumption of a conventional Vigenère cipher, he added a few more pages of unsuccessful investigations to his notes; and then – without any explanation or clue at all – his notes conclude with three pages of detailed description (folios 63-65), dated "*March 1846*", on how to decipher the remainder of the cryptogram applying as a third key the unusual name: "*Cacoethes*". Clearly, this name contains the trigram "*THE*" found earlier.

Did Babbage solve the body of Henry's cipher by a stroke of genius? I don't think so. Rather, all evidence point to the fact that he stopped further investigations as a waste of time and yielded to the plea in Henry's second letter of "*March 19, 1846*" (see figure 54).

Perhaps the most important reason that he should quit at this point was that in the course of iteration between probable keys and words, he had hit upon an equation (congruence) which to him appeared to be *the basic law of the Vigenère cipher*.

It turned up for the first time in the form (folio 51):

$$Trans = Cypher - Key + 1$$

and later again in two alternative formulations, which in his own handwriting are reproduced in figure 55 (folio 59). Judged by the nearest dated worksheets (folios 49 and 61), I would estimate that he put these equations on print some time in the period: February 21st to March 10th, 1846. The formulation turns up again a third time in his worksheets, but that appears to be several years later (folio 249). [24])

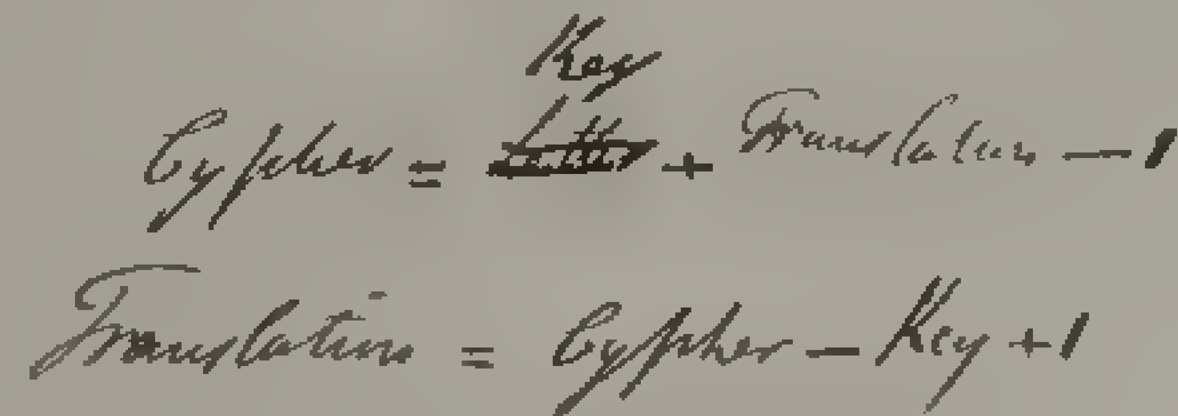


Figure 55. Babbage's formulation of the law of the Vigenère cipher. By permission of the British Library (Add.Ms. 37205, F. 59).

In view of our discussion in connection with figures 38 and 39, it is evident that the APL-function *TRY* implements Babbage's formulation in an 0-origin where, dropping the unit constant, it can be rewritten:

Translation = *Cypher* − *Key*
Key = *Cypher* − *Translation*

The symmetry of this formulation explains why a single APL-function will suffice to emulate his approach. Thus, depending upon our interpretation, the argument *GUESS* will play the role of either *Key* or *Translation*.

Babbage had in his possession various mechanical aids: cipher slides, discs and a cylinder, to facilitate the processes of enciphering and deciphering. [25] The cipher disc was invented by Leon Battista Alberti, an Italian renaissance engineer who much influenced Leonardo da Vinci. According to Morris Kline, he was "*the theoretical genius in mathematical perspective*". [26] Alberti described his invention of the cipher disc in a brief essay in Latin about 1466. [12] Undoubtedly, he was inspired by the methods he devised for surveying and map-making. First outlined in his *Description of the City of Rome*, the theme was later developed in his *Ludi Mathematici*, published 1450. In both of these works, Alberti employed a graduated circular disc with radial arm which, it has been suggested, he adapted from the astronomer's astrolabe. Thus, Alberti's instrument was an ancestor of the 16th century circumferentor, and so of the theodolite. [27] In this light, Alberti's invention of the cipher disc was not an isolated event. It was part of man's constant endeavour, as Babbage once expressed it, to throw mathematics into machinery.

In 1563, about a century after Alberti's invention, Giovanni Battista della Porta pointed out in his book: *De Furtivis Literarum Notis*, how a cipher disc could be developed into an equivalent tableau. This work Babbage completed by demonstrating that these different manifestations were but alternative representations of one and the same mathematical formulation, namely the one he had given in his law. Although Babbage first obtained this result explicitly in connection with his attempt to break Henry's cipher, the foundation was laid much earlier.

A generalization of Henry's choice of three consecutive keys, would be a key that changes continuously throughout the message. In his *Passages* Babbage mentions that, from "*a conversation which I had with the late Mr. Davies Gilbert, President of the Royal Society*", it became evident that both had imagined the same principle of using each cipher letter as the key for the following plaintext letter. A letter from Gilbert to Babbage, dated "*June 9th, 1833*", places this conversation in time. [28] It opens: "*I have not the least desire for inducing you to waste your time in unravelling my cypher, or the other aids* [?], *but mainly that you should convince yourself of its difficulty*".

Discussing this cipher, Babbage said, "*Although Davies Gilbert, I believe, and myself, both arrived at it from our own efforts, I have reason to think that it is of very much older*

date. I am not sure that it may not be found in the 'Steganographia' of Schott, or even of Trithemius". In fact, though, what they had come up with, was the *autokey*, Vigenère's invention which he originally described in 1586 in his *Traité de Chiffre*.

To start the enciphering process Babbage, like Vigenère before him, used a single letter as the so-called *priming key*. Babbage's explanation in his *Passages* runs as follows:

> "*This cipher was arranged upon the following principle: – Two concentric circles of cardboard were formed, each divided into twenty-six or more divisions.*
>
> *On the outer were written in regular order the letters of the alphabet. On the inner circle were written the same twenty-six letters but in any irregular manner.*
>
> *In order to use this cipher, look for the first letter of the word to be ciphered on the outside circle. Opposite to it, on the inner circle, will be another letter, which is to be written as the cipher for the former.*
>
> *Now turn round the inner circle until the cipher just written is opposite the letter A on the outer circle. Proceed in the same manner for the next, and so on for all succeeding letters.*
>
> *Many varieties of this cipher may be made by inserting other characters to represent the divisions between words, the various stops, or even blanks*".

Years later, while explaining this cipher to a friend, Dr. William Henry Fitton, who had asked Babbage's opinion of "*the possibility of making an inscrutable cipher*", then, as Babbage recounts in his *Passages*:

> "*... an indistinct glimpse of defeating it presented itself vaguely to my imagination. Having mentioned my newly-conceived doubt, it was entirely rejected by my friend. I then proposed that Dr. Fitton should write a few sentences in a cipher constructed according to this law, and that I should make som attempts to unravel it*".

After having spent some time on the cipher, Babbage "*found that it would not yield to my means of treating it; and on further examination I succeeded in proving that it was not written according to the law agreed upon*". Dr. Fitton, therefore, took the cipher back to his sister, Mrs. James, by whose aid it was composed,

> "*... and after the lapse of a considerable interval of time again returned, and informed me that I was right – that his sister had inadvertently mistaken the enunciation of the law. I now remarked that I possessed an absolute demonstration of the fact I had communicated to him; and added that, having conjectured the origin of the mistake, I would decipher the cipher with the erroneous law before he could send me the new cipher to be made according to the law originally proposed. Before the evening of the next day both ciphers had been translated*".

Unfortunately, Babbage's worksheets are too incomplete to permit us to recon-

struct his approach in detail. [29] Only one of the cryptograms is preserved, and he refers in his worksheets to *"trial by rules 1, 6, and 7"*, but no statement of these or any other rules are given. Some of his remarks are amusing: *"It now appeared that I was stupid for as ..."* (folio 7), and often spontaneous: *"Is the cypher wrong and law different ..."* folio 9, front). His concluding statement corroborates the account in his *Passages*, except for the fact that it is dated *"20 Feb. 1831"* (folio 9, back). Of course, Gilbert's letter of 1833 may refer to another cipher; or Babbage may simply have forgotten the actual course of events, as he was telling the story thirty years later.

The preserved cipher and a key to the lost one, reveal that the cipher alphabet merely was a shifted plaintext alphabet. So, at least on the point of a mixed cipher alphabet, Babbage was in error. Anyhow, what is interesting, is the fact that in actual practice Babbage was employing his law already then in that, guessing a word, he used the last cipher letters of the previous word as a priming key. Thus, his notes are filled with equations (congruences) of the same nature as those we found in connection with his solution of Henry's cipher almost fifteen years later. Of course, the important thing is that he did not make the general formulation expicit, even if the autokey does not differ in principle from the Vigenère cipher.

Anyhow, there can be little doubt that Babbage capitalized on his experience with the autokey problem, when he wrote down his explanation of the solution to Henry's cipher. In fact, by comparison with all his other unpublished material on ciphers, these three pages of description are perhaps his most complete. [30]

The first page which is reproduced in figure 56, is the most important. On it three distinct items are found. First, the cryptogram is rewritten to show beneath each word the repeated keyword, applied in the process, and its translation into plaintext. Secondly, it lists the standard alphabet with the letters numbered from 1 to 26. Thirdly, a series of three tables is given, pertaining each to one of the keys. Headed *"Table 1-3"*, each table is labelled by a number: *"6, 9, or 8"*, giving the number of letters in the keyword, and it further consists of two columns of numbers headed *"Rem"* and *"No. subtract"*, respectively. The first column *"Rem"* lists all the remainders modulo the number of letters in the keyword. The second column contains integers from the sequence: *"0-25"*. Evidently, these integers are the indices of the key letters in the plaintext alphabet, diminished by the value 1 and rotated cyclically, so that the index of the last key letter is aligned with the remainder 0.

A pencil note: *"To the Duke of Somerset"*, suggests part of its history. Yet, it is so unlike Babbage to document cryptographic material, that there must have been a very special reason for it. The most obvious explanation seems to be that it was his discovery of a basic law. Perhaps he felt that he ought to publish something about it if he ever got the time.

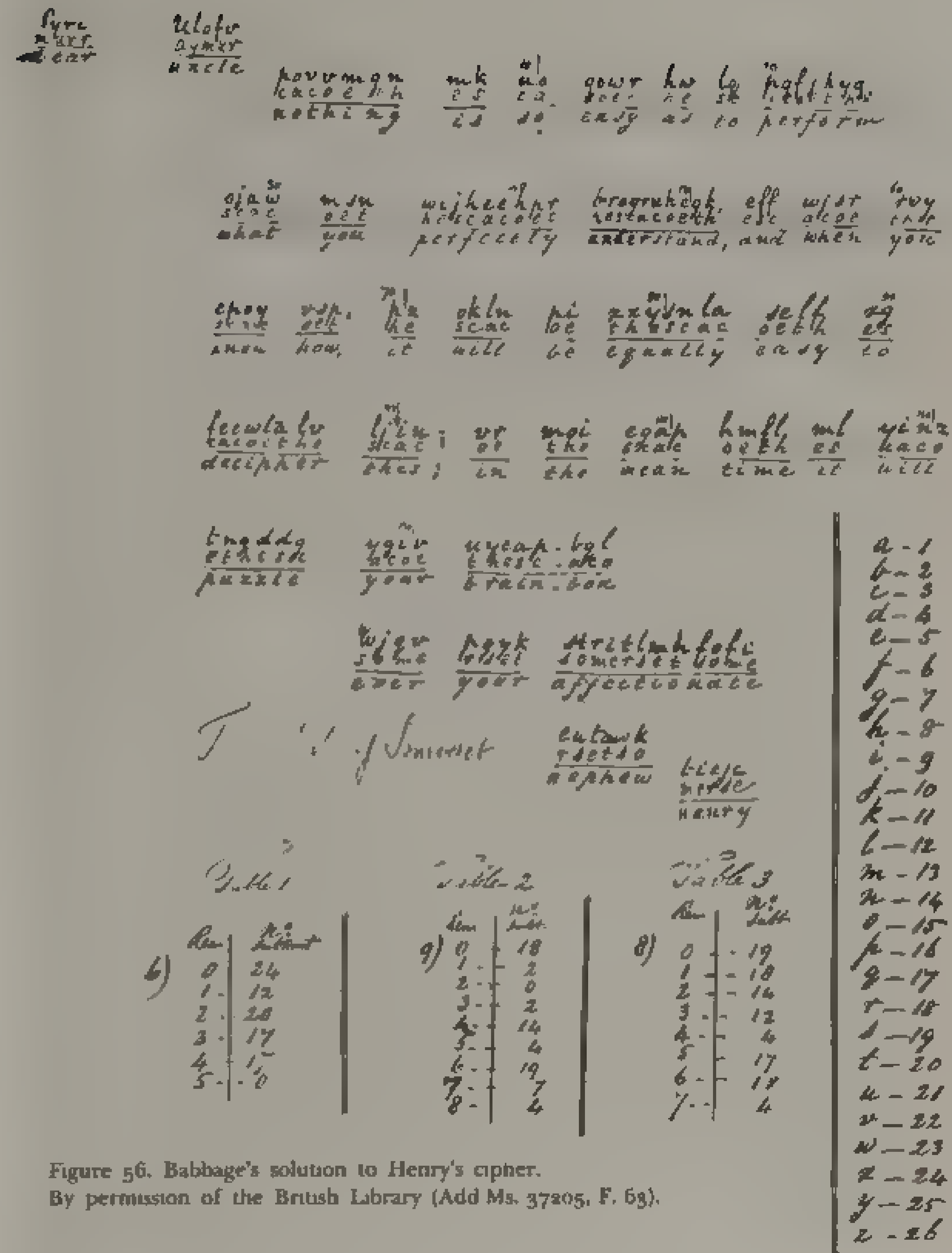


Figure 56. Babbage's solution to Henry's cipher.
By permission of the British Library (Add Ms. 37205, F. 63).

The remaining two pages are headed *"First key"* and *"Second key"*, respectively. In actual fact, they are concerned with each a different representation of the solution The two alternatives are a formulation in terms of arithmetic congruences, and a description of the use of a cipher disc, respectively.

The former is made up of three rules, written in ink and spaced apart to give room for a numerical illustration in pencil. In Babbage's own words, one might proceed as follows:

> *"Rule 1. Take the number of the cipher letter. Divide it by 9 and enter table 2 with the remainder. Against it in the table is a number.*
>
> *Example In the third line of the cipher take the first letter of the word MSN. The number of the cipher letter is 31. Divide by 9. Opposite the remainder 4 in Table 2 stands the number 14.*
>
> *2 Find the number in the alphabet corresponding to the cipher character.*
>
> *The cipher character is M which is the 13th letter in the alphabet.*
>
> *3. Subtract the number found in the table from the number last found. The remainder is the number in the alphabet of the letter to be found; if this number is negative* [read. non-positive] *add 26 to it.*
>
> *.. 13 − 14 = -1; add 26;* [result] *25 .. answers to Y, the letter of translation.*
>
> *. The other letters follow the same rule. Thus the two first words (first line) may be translated by the same rule using Table 1.*
>
> *The words in lines 7, 8, 9 may be translated by the same rule using Table 3".*

Clearly, this is a rather complicated manner Babbage has chosen to explain the use of his law. Undoubtedly, he endeavoured to come up with a non-mathematical description, or a user's manual. The real complication arises here from the fact that he is working in a 1-origin and, hence, forced to take into account the unit constant as well as the transformation of the principal remainder: zero to the value 26. These difficulties are in contrast to his far more simple description of the alternative approach, using a cipher disc. Here, he said

> *"On the fix't circle, called the* Letter Circle, *write the alphabet from right to left – on the movable circle, called the* Cipher Circle, *write the alphabet from left to right.*
>
> *To translate the cipher write the cipher key under the letters*
>
> *1 Take any cipher letter on the cipher circle and place it against "A" in the letter circle*
>
> *2. Then opposite the key letter on the cipher circle will be found its translation in the letter circle "*

To illustrate this procedure, Babbage took the second word *"MSN"* on line 3 together with its key fraction *"OET"*. Thus,

> *"Place the cipher letter "M" opposite "A" on the letter circle. – Then opposite the key letter "O" on the cipher circle will be found the letter "Y" on the letter circle, and similarly for the rest".*

Where, we may add, the plaintext word to be determined, is the word *"you"*.

The assignment of a *reversed alphabet* to the "fix't circle", may have been yet an observation inspiring Babbage to the formulation of, what has been called, his *"cryptographic equations"*. A cipher disc is basically an analogue computer performing addition by joining lengths end to end. Obviously, since subtraction is the converse operation, it may be executed by addition of the complement. That is, by addition of a reversed alphabet. Further, this explains why adding or subtracting a unit value in residue arithmetics, happen to represent the geometrical idea of a cyclic shift, to the left or to the right, in a mechanical apparatus.

The significance of Babbage's two descriptions: the arithmetic congruences and the geometrical notion of a cipher disc, was that he conceived them as alternative representations of one and the same abstract law. His use of a 1-origin indexing, made his mathematical formulation somewhat inelegant and his computational procedure inconvenient. Yet, the fact that he had arrived at all at a mathematical formulation of a law, was epoch-making In the history of cryptography, this contribution turned what hitherto had been an art, into a mathematical science. Unfortunately, Babbage did not publish, so his work made no impact at all

3.5 Laws on Laws

In 1888, seventeen years after Babbage's death and forty-two years after the formulation of his cryptographical law, another man independently contributed the same law, in a more elegant form using a 0-origin indexing and generalized to encompass also the Beaufort ciphers. This man was Marquis Gaëtan Henri Viarizio di Lesegno, whose name was gallicized to de Viaris. Born at Cherbourg in 1847 and a graduate of the famous École Polytechnique, de Viaris was commissioned in the Navy for a few years before he resigned at the age of twenty-five. According to Kahn [12]) he later became assistant police prefect and an infantry officer, and about 1890 he reorganized the Bureau de Chiffre of the Ministry of Foreign Affairs. Though, curiously enough, he signed himself as *"ancien officier de marine"* (retired navy officer) in his articles. He died in 1901.

De Viaris published his contribution in a series of articles in the *Génie Civil* [31]), but neither at the time, nor later did his ingenious formulation stir much interest In those days, former students of the École Polytechnique contributed a high-level scientific approach across the various fields of engineering, but often is was only appreciated by other graduates of the celebrated school. It was only in a longer

perspective that the impact made itself felt on society. Furthermore, the nature of cryptography is such that, by necessity, an appreciative audience must be small.

Based on our discussion up til now, it is a rather natural step that Babbage's formulation may be extended from the Vigenère cipher to those of Beaufort's and Beaufort's Variant. However, we must remember that de Viaris had to do it entirely on his own. Even more astounding is the fact that in the course of this work he discovered, presumably by symmetry considerations, that this family of ciphers had to include yet a member, hitherto unknown. [32]) This new cipher, which may well have been used in practice without being documented in the literature, is akin to the Vigenère cipher itself. For this reason, and to preserve a symmetry in the name-giving, I shall call it *Vigenère's Variant.*

De Viaris does not name this "new" cipher in his article, but neither does he speak of Beaufort's Variant. In fact, he only assigns names to, and acknowledges as known forms, the Vigenère and the Beaufort. Though, based on the key *Sebastopol,* he does illustrate the use of all four ciphers and also gives their laws. But he goes even further, for he combines the four laws into a single equation, his prominent *"l'équation cryptographique"*, common to the entire family of Vigenère ciphers. Paraphrasing Babbage's formulation, it may be written:

$$\textit{Translation} + \textit{Key} + \textit{Cipher} = \textit{Constant}$$

It is here understood, that one or more of the terms may be negative. The constant on the right hand side may be given alternative interpretations. Either, it may be considered a J-residue associated with a J-origin; or it may be conceived as a shift or a rotation of the alphabet, accomodating mathematically the carrier of a cyclic group, which we test by "running down the alphabet". Anyhow, without loss of generality, we shall simplify the following discussion by assuming that we only work in a 0-origin, so that we can assign the constant a zero value. That is, we consider the slightly more special situation:

$$\textit{Translation} + \textit{Key} + \textit{Cipher} = 0$$

Strictly speaking, of course, this is a congruence, and it should be written modulo the size of the alphabet. Though, the present formulation will serve for our purpose.

Basically, this equation or congruence is an invariant of a kind we have seen before. In particular, it resembles the equilibrium condition of vanishing forces that we discussed in connection with d'Alembert's principle. An even better analogy, I would suggest, is the physical law of energy conservation. Since the latter law is an equation, whereas the cryptographical law is a congruence, we have here what might be termed a *structural analogy.* Thus, rather than having the same mathematical model (conventionally associated with the term "analogy"), the present analogy is founded mathematically on an algebraic isomorphism, which exists between

simultaneous linear equations and simultaneous linear congruences with integral coefficients, for a fixed modulus.

But it is more than a mathematical similarity. As I shall now briefly try to demonstrate, it is also an *analogy in interpretation,* which in a procedural sense carries over into the manner of application. For this reason, I have dubbed de Viaris' generalization of Babbage's formulation: *The Conservation Law of the Message.* For the purpose of this law is to guarantee that, whatever form we give the message, it can always be unravelled. From this point of view, we may perhaps say that the law is the scientific restatement of Babbage's maxim *"that every cipher can be deciphered".* Mathematically, the law is clearly an invariant, and that which it preserves, is the message. However, let me begin by considering two properties of the physical law of energy conservation, which are of particular relevance to our discussion.

First, to preserve the invariant form of the physical law new terms have been added whenever the law failed. Through history this has given rise to a sequence of new kinds of energy: kinetic, potential, heat, electrical, chemical, etc., characteristic of the extensions to new distinct types of physical systems.

Secondly, the sign associated with each term in the law is defined arbitrarily as a particular characteristic of the distinct system configuration or interpretation. For example, since energy is a measure of mechanical work, a plus sign associated with the term of potential energy, signifies that this is the work which the mechanical system can supply to its environment. However, if a minus sign is introduced instead, the meaning of the term changes so that now it is the work which the environment (or external forces) can deliver to the system. In fact, to emphasize this change of meaning the negative of the potential energy is often called the "work function".

In cryptography, these two interpretational aspects have significant similarities. Thus, if we consider the three distinct terms of Vigenère's cipher: the plaintext, the cryptogram, and the key, analogous to the three energy terms of a mechanical system: kinetic, potential, and heat, then, adding a second key, introduces complications comparable to those of adding a fourth kind of energy, say electric, to the mechanical system. Similarly, if we change the signs of some of the three terms in the Vigenère cipher, this calls for new interpretations of the cryptographical system configuration, giving rise to the other ciphers in the family: Beaufort, Beaufort's Variant, and Vigenère's Variant. Yet, the similarity goes even beyond these conceptions.

As a scientific discipline, physics is divided into separate compartments: Mechanics, heat, electricity, etc., each described relatively to a reference frame of its own. The importance of the energy conservation law is that it provides a means – in fact, the only one – for tying these separate compartments together. To illustrate,

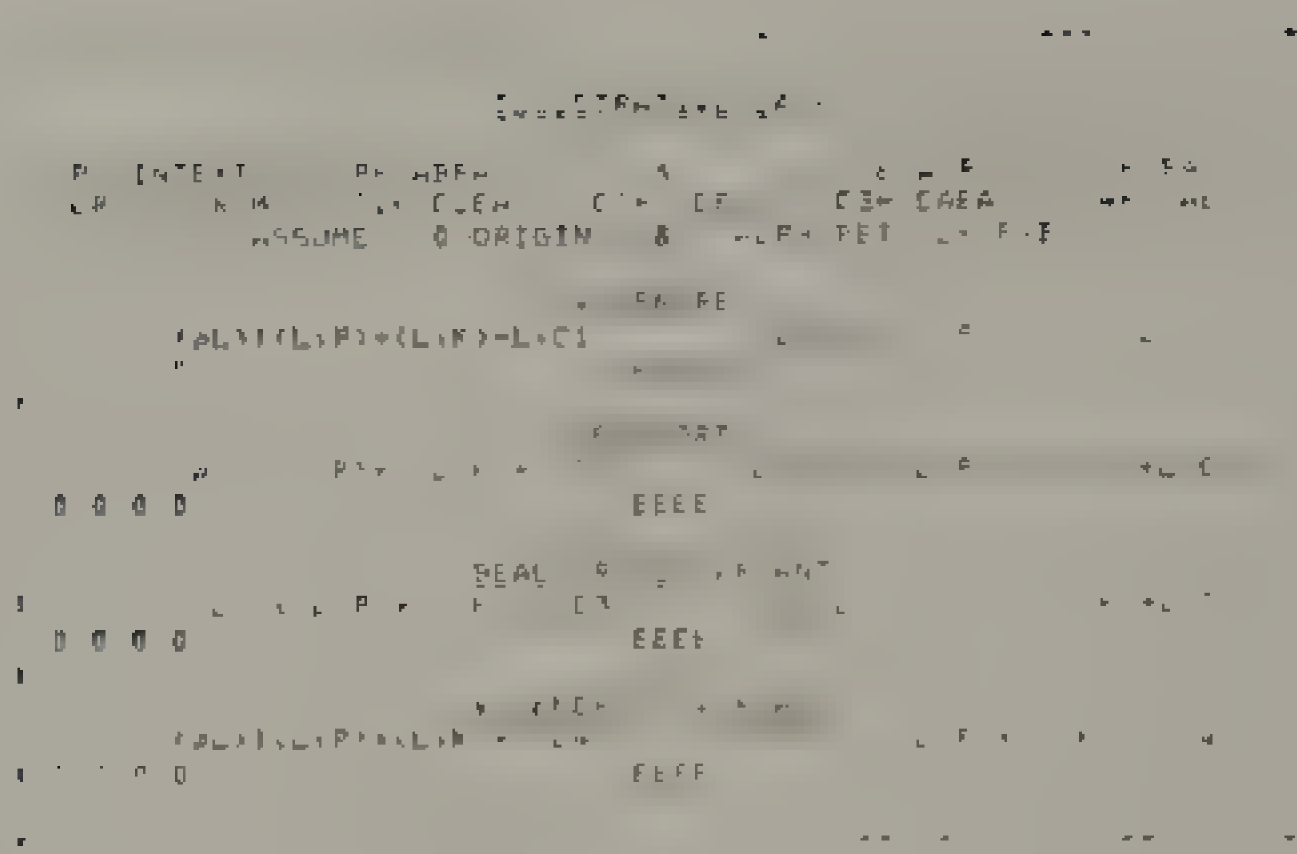


Figure 57. The conservation law of the message for the Vigenère family of ciphers.

for an electric motor, the law tells us how electrical energy is transformed into mechanical energy (work) and associated losses (dissipation). Yet, the choice of reference frame for the electrical subsystem (say, A.C. or D.C.) is completely independent of the geometrical reference used in measuring the mechanical torque.

The cryptographical law of conservation of the message, exhibits a distinct similarity in this respect. Thus, it ties together the three separate items: the translation, the key, and the cipher, but the choice of reference (alphabet) is made independently for each of these items, provided, of course, that they are all of the same size.

We shall not go any further on this point, since in cryptography the role of Babbage's and de Viaris' conservation law should by now be evident. A demonstration of this law for the various members of the Vigenère family of ciphers, is given in figure 57 assuming a 0-origin throughout.

Conservation laws, whether physical or cryptographic, are representative of the classical approach to science. They are closely associated with the phenomenon or system under consideration, and less amenable to a description common to some invariant operation or procedure as it is found in connection with a variety of phenomena or systems. For example, if we apply the conservation law of the message to the Vigenère cipher, the formulation is specific to this cipher. It tells us what we need to know about its encipherment and decipherment, but we have not the faintest clue whether or not the same processes are valid for Beaufort's Variant, say.

The "modern" approach, implementing Klein's Erlanger Program in terms of group theory, complements this classic conception by tracing invariant patterns "across the board", so to speak. We no longer deal with the individual phenomenon or system, but only with certain associated operations, which we investigate in the context of phenomena and systems in general. To illustrate, we may observe that encipherment for the Vigenère cipher and decipherment for Beaufort's Variant proceed by the same operation (see figures 48 and 49), so that it might be desirable to investigate this particular operation in the context of other cipher systems. Or, we may discover that addition or subtraction of congruent integers seem to have something to do with the spatial rotation of the multiplication table (see figure 39), so that considering the remaining rotations of the table, will perhaps provide an organized approach to the entire question of the operations of encipherment and decipherment. Thus, while the conservation law of the message accepts the signs of the individual terms as basically arbitrary, this conjecture might provide a new explanation derived from even more basic principles.

In all the mathematical sciences, from the pure to the applied, it is conjectures of this kind which captures the imagination of the innovators. For it is in questions such as these that we have the potential for further insight and understanding. This chain of questions and answers, which we call progress, provides in this case what appears to be an entirely new principle. Never before in our discussions have we established a group by submitting a multiplication table to reflections and other geometrical operations. A multiplication table was not an object under a set of operations. It was a representation of the results of such operations. Thus, we emphasized that group theory supplied the basic description of what happens when one kind of mathematical operation is performed on different elements, or when different operations are successively performed on a single element. Here, however, we are forced into a third interpretation which appears to constitute a further generalization of the last-mentioned approach, in that we let the single element be yet an operation, namely a multiplication table.

Figure 58 demonstrates this generalization for the Vigenère tableau of our standard example based on a four-letter alphabet. Whether enciphering or deciphering, we enter the appropriate transformation of the tableau by indexing, a so-called "table look-up". It is noteworthy, that Vigenère's Variant is the only cipher for which these two processes are associated with the same tableau transform. This explains its late discovery. For the other three ciphers, the tableau transform of encipherment differs from that of decipherment. Thus, we see how the group-theoretical approach cuts across the conventional description, captured cipher by

```
              +                                    +
                 T          ⁻100T        100T     100 100T
                  100T        T         100 100T     100T
                  100T      100 100T       T          100T
                100 100T      100T        100T         T
              +                                    +
                 F. KLEIN S   VIERERGRUPPE   (FOUR GROUP

                           ILLUSTRATIVE DATA

     PLAINTEXT     P← ABBA'       &          KEYWORD     K← BABE
     CRYPTOGRAMS   C1← CCEA    C2← ACEC    C3← CAEA    C4← AAEC
               ASSUME   0-ORIGIN   &   ALPHABET  L← EABC

                  KLEIN S GROUP OF CIPHER OPERATIONS

     ENCIPHERMENT          MULTIPLICATION TABLE        DECIPHERMENT

                               D←N←T
        VIGENERE             EABC                     BEAUFORT S VARIANT
      0 ONM[L⍳P,L⍳K]         ABCE                       0 ONM[L⍳C1,L⍳K]
  CCEA                       BCEA                 ABBA
                             CEAB

                               D←M←⁻100T
        BEAUFORT             EABC                        BEAUFORT
      0 ONM[L⍳P,L⍳K]         CEAB                       0 ONM[L⍳C2,L⍳K]
  ACEC                       BCEA                 ABBA
                             ABCE

                               D←M←⁻100T
    BEAUFORT'S VARIANT       ECBA                        VIGENERE
      0 ONM[L⍳P,L⍳K]         AECB                       0 ONM[L⍳C3,L⍳K]
  CAEA                       BAEC                 ABBA
                             CBAE

                               D←M←⁻100 100T
    VIGENERE S VARIANT       ECBA                   VIGENERE S VARIANT
      0 ONM[L⍳P,L⍳K]         CBAE                       0 ONM[L⍳C4,L⍳K]
  AAEC                       BAEC                 ABBA
                             AECB

                     THE VIGENERE FAMILY OF CIPHERS

   METHOD    |  CONSERVATION LAW     |   ENCIPHERMENT     |   DECIPHERMENT
             +                       +                    +
  VIGENERE   | 0 =   P  +   K  - C1  | C1 =   P  +   K    |  P  =   C1  + (-K)
  BEAUFORT   | 0 =   P  + (-K) + C2  | C2 = (-P) +   K    |  P  = (-C2) +   K
  B S VAR    | 0 = (-P) +   K  + C3  | C3 =   P  +  -K    |  P  =   C3  +   K
  V'S VAR.   | 0 =   P  +   K  + C4  | C4 = (-P) + (-K)   |  P  = (-C4) + (-K)
```

Figure 58. Encipherment and decipherment by a Vigenère tableau under Klein's four-group: D_2

```
  DEFINE CYCLIC GROUP  C2.  WITH NEGATION OF ALPHABET AS GENERATOR
                  ⌽              L[ ⍴L) ⍳L⍳L)                   100L
        EABC                ECBA                           ECBA
  ASSUME   0 ORIGIN       PLAINTEXT  P←'ABBA',     &     KEY  K← BABE

                          THE DIRECT PRODUCT GROUP

        MODULO ARITHMETIC                            CIPHER DISC OPERATIONS

        L[(⍴L)|(L⍳L)∘.+L⍳L]                          T[L⍳L,L⍳L]
  EABC                                      EABC
  ABCE                                      ABCE
  BCEA                                      BCEA
  CEAB                                      CEAB

        L[(⍴L)|(-L⍳L)∘.+L⍳L]                         T[(⌽100L)⍳L,L⍳L]
  EABC                                      EABC
  CEAB                                      CEAB
  BCEA                                      BCEA
  ABCE                                      ABCE

        L[(⍴L)|(L⍳L)∘.-L⍳L]                          T[L⍳L,(⌽100L)⍳L]
  ECBA                                      ECBA
  AECB                                      AECB
  BAEC                                      BAEC
  CBAE                                      CBAE

        L[(⍴L)|(-L⍳L)∘.-L⍳L]                         T[(⌽100L)⍳L,(⌽100L)⍳L]
  ECBA                                      ECBA
  CBAE                                      CBAE
  BAEC                                      BAEC
  AECB                                      AECB

                          ENCIPHERMENT OPERATIONS

        VIGENERE                                     VIGENERE
        0 ONL[(⍴L)|(L⍳P)∘.+L⍳K]                      0 ONT[L⍳P,L⍳K]
  CCEA                                      CCEA
        L[(⍴L)|(L⍳P)+L⍳K]
  CCEA
        BEAUFORT                                     BEAUFORT
        0 ONL[(⍴L)|(-L⍳P)∘.+L⍳K]                     0 ONT[(⌽100L)⍳P,L⍳K]
  ACEC                                      ACEC
        L[(⍴L)|(-L⍳P)+L⍳K]
  ACEC
        BEAUFORT S VARIANT                           BEAUFORT S VARIANT
        0 ONL[(⍴L)|(L⍳P)∘.-L⍳K]                      0 ONT[L⍳P,(⌽100L)⍳K]
  CAEA                                      CAEA
        L[(⍴L)|(L⍳P)-L⍳K]
  CAEA
        VIGENERE S VARIANT                           VIGENERE S VARIANT
        0 ONL[(⍴L)|(-L⍳P)∘.-L⍳K]                     0 ONT[(⌽100L)⍳P,(⌽100L)⍳K]
  AAEC                                      AAEC
        L[(⍴L)|(-L⍳P)-L⍳K]
  AAEC
```

Figure 59. Encipherment by a Vigenère tableau under the direct product group: $C_2 \times C_2$.

cipher in the conservation law. The emphasis has moved from invariance of the individual system design to invariance of the processes or operations to which the entire class of systems submits.

The group under which the operations on the Vigenère tableau are invariant, is known as *Klein's Vierergruppe*, or the four-group, or quadratic group. Technically, it is called the *dihedral group*, D_2. The word "dihedral" refers to "two planes". The reason for this, is that this class of groups describes the congruence motions of a regular polygon, such as it is caused by two generators, referring each to a symmetry about a plane. The subscript, here 2, denotes the number of vertices in the polygon associated with the group. The order or number of elements of a dihedral group is always twice the number of vertices in the associated polygon. It may be mentioned that the only other group of order 4 is the cyclic group C_4

Although our generalization is clearly mathematically correct, it is deficient in a theoretical sense. It does not rest on those fundamental principles of invariant scale-forms that we consider basic to our geometrical conception of data. We therefore have to reconsider our entire approach

A clue to a revision, is the observation that either of the group generators is a composite APL operation, combining a reversal with a cyclic shift. This was also one of the fundamental operations which, discussed in figure 40, preserved the ordinal scale-form. Since basically the Vigenère tableau is the outer product of an alphabet by itself, it is now obvious that we shall reinterpret the operations on the Vigenère tableau as derived from order-preserving operations on the alphabet. Here, a handy information found in any mathematics textbook dealing with group theory, is that Felix Klein's four-group is the direct product of the cyclic group of order two by itself·

$$D_2 = C_2 \times C_2$$

Introducing this fact, we find, as demonstrated in figure 59, that instead of our proposed generalization performing operations on a multiplication table, the correct interpretation is that we combine order-preserving operations on one alphabet with corresponding operations on another alphabet. [55]) Thus, the criterion of a correctly developed theory for the Vigenère cipher family, is that the results are consistent also in a "physical" sense with our basic notion of data as determined by their scale-forms. The two representations of the direct product in the figure, put in perspective Babbage's corresponding two explanations of his solution to Henry's cipher. His remarkable intuition drove him beyond his formulation of the conservation law towards a description of the operations, subdivided structurally into two similar parts: One for the residue arithmetic and another for the geometrical motions on the cipher disc. It is exactly this similarity that is captured by the two representations of the direct product group in figure 59.

As an undergraduate at Cambridge, Babbage went into a compact with his two close friends, John Herschel and George Peacock, that they would "*do their best to leave the world wiser than they found it*". His work, even on ciphers, demonstrates that he took this vow serious

3.6 Foreign Supremacy

In connection with his discussion in 1819 of the Vigenère cipher, Lindenfels, in a note, warned his readers against using short keywords because,

> " *in long dispatches, one is far too often faced with the necessity of repeating it, so that several times it becomes possible that one or another cipher letter will designate one and the same plaintext letter, and, hence, provide the experienced decipherer with an opportunity for making discoveries*"

This problem of using the periodicity of the key to break a cipher, is central to the public exchange of letters in 1854, in the Journal of the Society of Arts, between John Hall Brock Thwaites, a surgeon and dentist of Bristol, and Babbage; the latter writing anonymously under the signature: "C"

This exchange of letters is fascinating on several accounts. Being Babbage's only publication in the field of cryptography, it bears testimony to Babbage's professional skill and ability. By his ingenious solution developed together with his youngest son Henry Prevost, it precedes by almost a decade the famous and now standard Kasiski method published 1863. [22]) The extrication of Thwaites' two keywords: "*TWO*" and "*COMBINED*", used successively in a double encipherment, is crowning evidence to our story of Babbage's mathematical approach to cryptography in particular, and data in general. But this exchange of letters has also a human side.

On the surface, to be sure, this part of the story has the ordinary ring. A well-meaning, somewhat ambitious and rather headstrong amateur, crushed without mercy as a mere dilettante. Unbelieving to begin with, he is gradually stunned by the hard facts. Yet, growing in defeat, he bows out gracefully, his high hopes in ruins, but a wiser man

However, there is also an inside story. Open-ended, it took place in the higher circles of society with connections even to the Foreign Ministry. Whether Babbage got entangled by accident or by request, is not clear, but in the course of events he came to see himself as an advocate if not a champion of a higher cause. To him, as a principle, it became a matter of defending science and upholding its highest standards. Surely, his involvement was a well known secret to many who had witnessed his battle with the Royal Society, so his reputation was at stake. He had

to win and, having the opportunity to do so triumphantly though without showing off, he did it with éclat. For his exit line, concealed in his unanswered counter challenge to Thwaites, was the two keywords: "*FOREIGN SUPREMACY*".

It is in the nature of the facts of this story that, to appreciate it, one has to read this exchange of letters. These letters are therefore reproduced in extenso in figure 60 (pp. 253-258), from the old pages of the Journal of the Society of Arts. [34] To explain the factual content of Babbage's approach, it will be simulated in the APL terminal session. I therefore, the emphasis here will be on the facts I have been able to unearth concerning the human side of the story. However, to prepare for the APL presentation, it is desirable that the letters are read in the broader perspective of the physical notion of harmonic analysis, to which topic they form by analogy a fascinating introduction. A brief orientation on what we understand by harmonic analysis, is therefore in order.

In an article in Encyclopaedia Britannica entitled "*Harmonic Analysis*", a contemporary of Babbage's, James Clerk Maxwell (1831-1879), the great physicist, opens his description by this statement: [35]

> "*Harmonic Analysis is the name given by Sir William Thomson and Professor Tait in their treatise: 'Natural Philosophy', to a general method of investigating physical questions, the earliest applications of which seem to have been suggested by the study of the vibrations of strings and the analysis of these vibrations into their fundamental tone and its harmonics or overtones*"

In physics and engineering, harmonic analysis is the study of waveforms or, to express it mathematically, of periodic functions. Here, Fourier's powerful quantitative methods come to mind, but we should realize that the topic may be given a far broader interpretation, extending into the domain of linear congruences. Thus, in his article Maxwell points out:

> "*The harmonic method may be defined in a more general manner as a method by which the solution of any actual problem may be obtained as the sum or resultant of a number of terms, each of which is a solution of a particular case of the problem. The nature of these particular cases is defined by the condition that any of them must be conjugate to any other*",

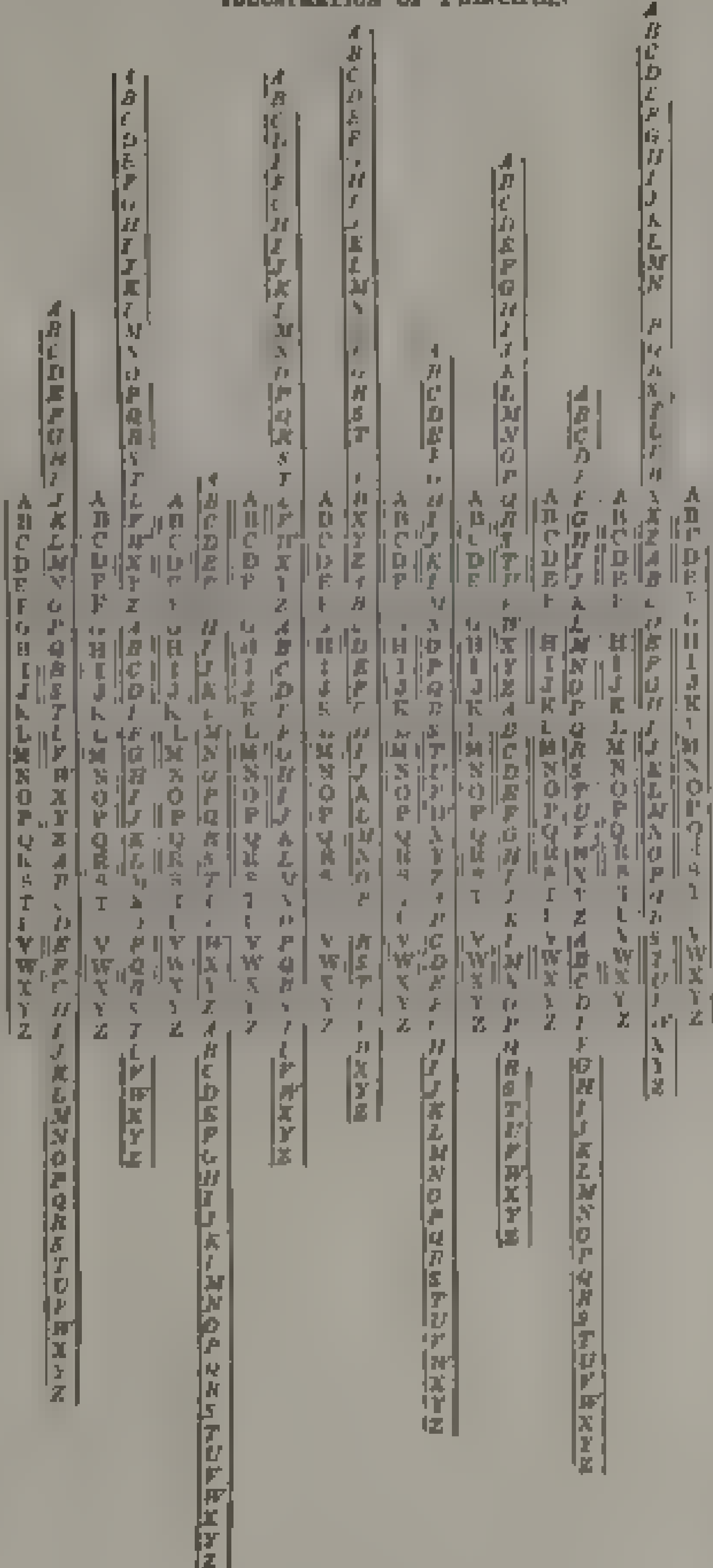
As applied here, the term "conjugate" is explained by Maxwell

> "*When two modes of motion of the same system are conjugate to each other, the existence of one of them does not affect the other*".

Basically, the problem under discussion in the Journal of the Society of Arts, is one of harmonic analysis in this broad sense of Maxwell's. By analogy to radio

JOURNAL OF THE SOCIETY OF ARTS

ILLUSTRATION OF PRINCIPLE.



SECRET, OR CYPHER WRITING

SIR,—Permit me, through the "Journal of the Society of Arts," to make known a system of secret (or cypher) writing I have lately invented and patented the apparatus and to enclose, for the acceptance of the Society, the apparatus devised for its practical application, which, I believe, will be found to answer all the purposes intended. It is formed, as you perceive, of a series of fixed alphabets printed in *black* letters, and these alternating with another series of double alphabets in *red* letters*; the latter moving in grooves. By this arrangement you can, at pleasure, form any word or words in a line with any letter on the fixed alphabets; for instance, you wish to form the word *telegraph* against K. Begin at the left hand, bringing *T* to the black K, then the next slide move down until *E* is opposite the second black K, and so on until you spell the word, removing the last slide, which is not required. This is the *key word* to any writing you may wish to send; thus, you desire to communicate the sentence "I have had an interview." Begin by spelling from left to right, using the red letter as the cypher, opposite the I you find *R* the H *B*, A *B*, V *P*, E *A*, H *O*, A *Q*, D *I*, A *X* (then return to the left, and proceed N *W*, I *O*, N *O*, T *A*, E *A*, R *Y*, V *L*, I *A*, E *B*, W *F*, consequently, the cypher of this message would appear as R B B P A O Q I X W O O N A Y L N B F, which may be read by the party to whom it is sent, by fixing his key word as you did, viz., *telegraph* against K; he reads it by finding the first letter on the red alphabet, and using the black one against it, and so on. It will be seen that, even in this short message, the letter A is represented by *B*, *Q*, and *X*. *B* also represents H, A, and E. I, again, is represented by R, O, and N, and thus leaves no clue to the deciphering, which I feel certain is impossible unless the key-word is known. The same sentence written in the key of *microscope* against U would appear thus:—*A*, *V*, *I*, *S*, *Y*, *F*, *I*, *X*, *B*, *X*, *A*, *B*, *V*, *B*, *LT*, *Q*, *Y*, *R*, in this the three *B*'s are together, representing N T E. You may thus vary your cypher *ad infinitum*, and each variation equally unable to be deciphered without the key, but with it is as equally easy. It must be at once apparent that the complexity may be much increased by permutating (on well-known principles) each of the moveable alphabets, and in many other ways; but, in its simplest form, which I have described, I believe it will be found as complete as need be. Of course, the reading and writing may be indifferently from the fixed to the moveable, or the contrary, from left to right, or

* The red letters are here represented by the capitals in italics. Of the four examples which Mr Thwaites refers to, it has been considered necessary to illustrate only one.

Figure 60. Mr. Thwaites' cipher. Courtesy the Royal Society of Arts.

the reverse, in fact, there is no limit to its variations, and which may be agreed upon by the parties corresponding. You can with the article apparatus now sent, use a key to the extent of twenty letters; thus, your key is *physically impossible;* spell two letters at a time, using both the fixed and moveable alphabets. Sentences as keys may be used in like manner, and to any extent.

I need hardly observe that this system is applicable to any language. Its uses must be obvious to all, and the further employment of that useful help at the present day (the electric telegraph) certain, for by its means messages of the most private character may be sent, and not a chance of discovery. This fact I have proved, as by that I communicated with my friend Mr. Coathupe, addressing him from London and on the same day, July the 20th, sent to the *Times* a short note, which appeared on the 2 st. in the second paragraph, second column; it is this:—
G Z Z E S, G V, T N S R X W Y F U O, L X W V, Q B O J Z, F X H F J B X, Q X N O Z K O, S O, E R T G Y B M F X Y—D U O B, S L U P, T A O B V J P T Q R S I W, I T Z, S D E J P L M O F F, Z U G Q S C G *V B B V*., which interpreted by the use of the key word *Minerva* against H will thus read:—
"By this communication I claim precedence in the discovery of secret correspondence on the principle of permutation." The *V B B V*, is read by *J H B T* (my initials), as key from right to left against H; it then is proved to be J. H. B. T. It will thus be seen that this system may be used for establishing claims where publicity is not at first desirable.

To all public bodies, who are in the habit of enquiring by telegraph, it is evident it must prove useful, for, at most times, such enquiries are necessarily confidential; and to private parties at a distance from each other, it will prove a means of sending messages that are desired to be kept sacred to the parties communicating—and are there not many such cases? I might multiply instances without number where such a system will I trust prove a boon.

Thanking you for the space afforded me in your valuable journal.

I subscribe myself, yours faithfully,
JOHN H. B. THWAITES.

17, Park Street, Bristol, August 10th, 1854.

MR. THWAITES'S CYPHER.

SIR,—The cypher in the Journal is a very old one, and to be found in most of the books; it is not an easy cypher, but it has very often been deciphered under a more difficult form.

The patent rods are not new, I, and I believe, most other decipherers have had them in pasteboard for thirty years. I have them also in box-wood. I have also the same thing in a series of pasteboard circles, moveable round a common centre, each circle having on its circumference the twenty-six letters of the alphabet.

The best form is, perhaps, rings of box-wood placed side by side on a cylinder, and having the twenty-six letters on the circumference of each. I have also invented alphabets. The great use of the rods, &c., is to save time in deciphering.

You will, most probably, recognise the cypher if put into another form.

In the subjoined table the key of the cypher is j u b o w h q f x

Mr. Thwaites's Cypher . . . j u b o w h q f x j u b o w h q f x j—Key.
R B B P A O Q I X W C O N A Y I N R Y
i h a v e c h e d a n a l s t e r v l e e—Trans.

	j	u	b	o	w	h	q	f	x
A	r	g	z	g	e	t	k	v	d
B	s	h	a	h	f	u	l	w	e
C	t	i	b	i	g	v	m	x	f
D	u	j	c	j	h	w	n	y	g
E	v	k	d	k	i	x	o	z	h
F	w	l	e	l	j	y	p	a	i
G	x	m	f	m	k	z	q	b	j
H	y	n	g	n	l	a	r	c	k
I	z	o	h	o	m	b	s	d	l
J	a	p	i	p	n	c	t	e	m
K	b	q	j	q	o	d	u	f	n
L	c	r	k	r	p	e	v	g	o
M	d	s	l	s	q	f	w	h	p
N	e	t	m	t	r	g	x	i	q
O	f	u	n	u	s	h	y	j	r
P	g	v	o	v	t	i	z	k	s
Q	h	w	p	w	u	j	a	l	t
R	i	x	q	x	v	k	b	m	u
S	j	y	r	y	w	l	c	n	v
T	k	z	s	z	x	m	d	o	w
U	l	a	t	a	y	n	e	p	x
V	m	b	u	b	z	o	f	q	y
W	n	c	v	c	a	p	g	r	z
X	o	d	w	d	b	q	h	s	a
Y	p	e	x	e	c	r	i	t	b
Z	q	f	y	f	d	s	j	u	c

The letter in the cell of the first vertical column j opposite to R is i
Ditto u B is h
Ditto b B is a
Ditto o P is v
Ditto w A is e, and so on

In cyphers the smaller the number of words the longer the time required for detection.

If the words are not separated, or falsely separated, a longer time is necessary.

It may be laid down as a principle that it is never worth the trouble of trying any inscrutable cypher unless its author has himself *deciphered* some very *difficult* cypher.

C.

SECRET OR CYPHER WRITING.

SIR,—In reply to your correspondent "C's" communication in the Journal of September 1st, wherein he asserts that my cypher is not new. I must in the first place beg to ask him in what book he has seen described a similar one: not that for a moment I claim the invention of double alphabets, for either cyphering or decyphering, but I do claim the priority of invention in the form in which I have put them, whereby a *key word* (*or words*) *in conjunction with a letter* may be used to the extent I have shown, and still maintain that simplicity without which it would be comparatively useless, or rather, I should say, unused. I have never myself seen any other apparatus by which any number of words may be used as keys, and without the necessity of making arbitrary forms; when I say any number of words, I mean that any number of persons may use different words in their communications, and still the apparatus be perfectly applicable. On this was based the patent I took out, but the most simple form which I have only as yet described, was *worked down* from *several* much more complex ones, and I believe *all new*. The next in succession I will now attempt to describe.

I form a permutated alphabet for each letter of the twenty-six, every one having *its own permutation*, and with these I spell the key-word from right to left, (or the reverse) using the permutation answering to each letter. I then spell, as before described, the key-word from left to right (or the contrary), against the key-letter as before, and by this means complicate the matter most materially; in fact, let your correspondent "C" refer to De Morgan's "Essay on Probabilities," and he will then perhaps allow, that by this arrangement the decyphering is quasi impossible. I will thus put the question.

What are the chances of the arrangement of (we will say) seven letters out of the twenty-six, either from right to left, or the reverse, being found out? and when this is calculated then again comes the value attached to each letter in the shape of the permutation and after that, the further decyphering which "C" acknowledges is *not* easy, and if he refers to your Journal in which I first described my cypher, August 11th, I there said, "that each alphabet could be permutated on well-known principles, but that I believed the most simple form would be sufficiently complex for all practical purposes;" and *this opinion I still maintain*.

I will here put another question to your correspondent "C." Suppose, in the arrangement previously described, I cyphered a communication according to my plan, in a word of ten letters, with a key-letter, and then cyphered *that* cypher so obtained in a word of nine letters, with another key-letter, what reasonable probability is there of his finding out the value of the last cyphered one?

I know not whether you have observed in "C's" letter that he has formed an arbitrary table (and this arrangement, by the bye, he is indebted to a *lady's* invention for), founded on my own key-word, Telegraph, against *k*, using the *arbitrary* letters that appear against *a*; this can be at once rendered apparent, by fixing on my apparatus the word telegraph against *k*; it will then be seen that "C's" key appears against *a*, as T U B U W H Q F X. Is it, I may well ask, fair, that my weapons should thus be used so as *apparently* to depreciate my invention? I think not. Of course every communication must perforce have twenty-six keys, but *only one* intelligible and easily remembered. The great advantage of using an *intelligible* word is, that it may be understood by correspondents, that the last word (or otherwise) of a communication may be used as the key to the next forwarded.

Allow me to refer you to the June number of the "Quarterly Review," page 148, where it is remarked—"At all events some simple yet secure cypher, easily acquired and easily read, should be introduced, by which means messages might to all intents and purposes be 'sealed' to any person except the recipient. We have reason to believe that Professor Wheatstone has invented a cypher of this description *which has not yet been made public*." I ask you whether the one I have introduced does not answer the required conditions? *and, if not*, would it not be desirable that a better should at once be made known.

I cannot at all understand how your correspondent "C" can know what I have patented,—*certainly not* what he calls the "patent rods." I should, indeed, be wanting in sense to patent that which, as a schoolboy, I knew and used at least thirty years ago. What I have patented will be made public when my full specification is out, and not before; and it strikes me that the best opposition he could have offered would have been in the usual way, viz., opposing the patent; and for this purpose plenty of time has been given, and in that field also I should have been happy to have met him. In the first instance I made a free offer of my invention in a quarter where I had every reason to believe such a system was *required*; it was refused, and it was *then* I was induced to patent it for my own protection. I cannot say I regret it, for within this week I received the following from one of our first merchants here:—

"A merchant in Bristol enters into an agreement or contract with a merchant in Liverpool. The merchant in Liverpool is supposed to be in difficulties, and the friends of the Bristol merchant wished to communicate the fact to him, but not liking the idea of communicating so important a fact to him by *Telegraph* openly, (and such a communication the Telegraph company will not send) had no resource but to write by post. This caused a day's loss, and before the reply could arrive, the bankruptcy of the contractor was too certain.

"If some means of communication could be resorted to by which *such important matters* could be imparted without exposure, it would be of the utmost value, and, as in the above instance, the twenty-four hours saved may prove of essential importance."

On another point allow me to ask you, sir, if no slight saving could be effected in the expense of Queen's Messengers? not only in money, but especially in time. An *inscrutable* cypher message may be sent to Vienna and repeated back in less than six hours. May not this prove of paramount importance, especially at this time, and to prove that I can show an inscrutable one, I cypher the following few lines from the first act in the "Tempest":

"Soft, sir, one word more,
They are both in either's powers: but this swift business
I must uneasy make, lest too light winning
Make the prize light. One word more, I charge thee
That thou attend me, thou dost here usurp
Upon this island as a spy, to win it
From me, the lord on't."

It is thus cyphered:—

UTMU, DQV, UKS, LKZT, LRWN, FLHL, HPG, SVUS, QR, KFRWAZL, ORBNDW, EHA, RJZZ, THQJZ, YHEVUBV, N, VGWW, HUCJIF, NLSI, RBGL, PWE, KLLQF, ALAUGPX, TBVM, XNB, DGBBI, KLLQF, SQR, LMTU, TPCM M, IDGGM, JGHJ, GTEW, LGMW, KAUPVB, SB, HWKG, TNVY, QQVH, BZSTG, BQZV, XNFG, XOTQMG, FB, M, WSL, AM, YZU, JE, NVOJ, AT, PPC, KBWM, ARW.

Acquired the key of the above (which is simple and one that a child might understand and use), and the only apparatus used is exactly like the one I forwarded to you, and described in a former number of the Journal, and if so difficult as I believe, to find the key, how much must the difficulty be increased to decypher when the translation is not given, yet even this is not nearly the most difficult form in which I could put it, but I again reiterate that the most *simple form* is amply sufficient for all practical purposes. As regards your correspondent "C.'s" last paragraph in his letter, our opinions are so widely different on the subject, that it needs no comment from me.

Professional engagements quite prevented my answering "C.'s" letter last week, and now thanking you for so much space in your valuable Journal,

I subscribe myself, yours faithfully,
JOHN H. B. THWAITES.

17, Park-street, Bristol, Sept. 11th, 1854.

MR. THWAITES'S CYPHER.

Sir,—Mr. Thwaites rests the value of his *inscrutable* cypher on the impossibility of finding its key, even when both the cypher and its translation are given. He quotes a passage from "The Tempest," and gives the same in cypher. The best answer is at once to print the master-key of that cypher.

To interpret any character in the cypher:—

Count its number from the beginning. Divide this number by 24, and take the remainder. Opposite that remainder in the annexed table is found a Tabular number.

Remainder.	Tabular Number	Remainder.	Tabular Number
0	24	12	22
1	2	13	8
2	17	14	16
3	7	15	20
4	1	16	3
5	11	17	5
6	6	18	9
7	4	19	12
8	6	20	4
9	23	21	3
10	14	22	13
11	15	23	7

Subtract the Tabular number from the number expressing the place of the cypher in the natural alphabet. This last remainder will then express in that alphabet the place of the letter, which is the translation of the given cypher character; when this difference is negative, add twenty-six to it.

Thus—take the word "thou" (represented in the cypher by *gowo* and *hwkc*) which occurs twice in the fifth line.

g is the 142nd character. 142=5×24+22
opposite this remainder 22 is the Tabular number 13.

The cypher *g* is the 7th letter in the natural alphabet.

Then . . . 7 = place of cypher in the alphabet.
Subtract . . 13 = Tabular number.

Last remainder— 6
Add . . . 26

20 the 20th letter of the alphabet is *t*.

The cypher o (the 15th letter of the alphabet) is the 143rd character. 143=5×24+23. The remainder 23 gives the Tabular number 7.

Then . . . 15 = place of cypher in the alphabet.
Subtract 7 = Tabular number

8 the 8th letter of the alphabet is *h*.

The cypher *w* (the 13th letter) is the 144th character. 144=6×24+0. Remainder is zero, which gives the Tabular number 24.

13 = place of cypher
Subtract . . 24 = Tabular number.

—11
Add . . . 26

15 15th letter of the alphabet is o.

The cypher *w* (the 23rd letter) is the 145th character. 145=6×24+1. Remainder = 1 which gives Tabular number 2.

Then . . . 23 = place of cypher.
Subtract . . 2 = Tabular number.

21 the 21st letter of the alphabet is *u*.

In the word *hwkc*,

Cypher *h* (8th letter) is the 154th character. Remainder = 10, which gives Tabular number 14.

8 = place of cypher
14 = Tabular number.

—6
Add . . 26

20 20th letter of the alphabet is *t*.

Cypher *w* (23rd letter) is the 155th character. 155=6×24+11. Remainder = 11, which gives Tabular number 15.

Then . . . 23 = place of cypher
15 = Tabular number

8 8th letter of the alphabet is *h*.

Cypher *k* (11th letter) is the 156th character. 156=6×24+12. Remainder = 12, gives Tabular number 22.

Then . . 11 = place of cypher
22 = Tabular number

—11
26

15 15th letter of the alphabet is o.

Cypher *c* (3rd letter) is the 157th character. 157=6×24+13. Remainder = 13, gives Tabular number 8.

3 = place of cypher.
8 = Tabular number.

—5
Add . . . 26

21 21st letter of alphabet is *u*.

Mr. Thwaites seems not aware of the principles on which such cyphers are constructed, for he appears to have employed two cyphers in succession, viz., the word TWO against *p*, and COMBINED against *c*.

The first is a common cypher of three alphabets, recurring at equal intervals, indicated by the word TWO. The words LOG or RUM would do equally well. The cypher thus arrived at is then translated into another cypher of the same kind, having eight alphabets, and indicated by the word COMBINED against *c*.

It seems to have escaped Mr. Thwaites's notice, that the several successive translations add nothing to the security but much to the labour of his cypher. He will find below the first line of his quotation translated into those two cyphers, and will perceive that the order in which they are made does not alter the result:—

Soft, Sir, one word more by TWO against *p*
wvex ahv vml dnvk lsyd by COMBINED against *c*
ulmu dqv uks lkzt lrwn

Soft, Sir, one word more by COMBINED against *c*
qyng wrr nlo elvm mnpo by TWO against *p*
ulmu dqv uks lkzt lrwn

The same result will be given by the master-key above with one translation. The second letter T in Mr Thwaites's cypher is a mistake: it should be F.

Mr. Thwaites strongly protests against the received rules amongst decypherers, viz., that no one has the privilege of proposing a challenge cypher except he is himself known to have deciphered a difficult cypher.

This rule is founded on common sense, and is admitted, because it is perfectly well known that it requires a very small exertion of intellect to contrive a very difficult cypher. But to contrive a very difficult cypher, which is also very easily written and as easily translated, requires an understanding which has mastered all the principles of deciphering. Having accepted Mr Thwaites's challenge, and having sent you the solution, I am now in a position to call on Mr. Thwaites to try a cypher of my own. I shall, however, at present content myself with asking him to do what I have already done for him, namely, from the same passage of Shakspeare, cyphered according to his own law, to discover my key.

Jcze wil hdx fvow lguq onka wos vnigo fx wadgzjlt oa jhow gpavrg vanfi hez d ajj n afw coclez zafe cqkx dwm mekrg xixxad xkrh nxch itpvw ogtxy yeu cuig cqzt fcxtev w xm kkng xquq sa n r gexs taaq wml pdon zraa focv gqxdmxu q eab ry ax hw tkqp ze gub iyrh wjk.

I have the honour to be, &c.,

C.

October 2, 1854.

P.S. In my last note, printed in your issue 1st September, there is a curious mistake. The sentence there appears thus:—"I have also invented alphabets. It should be, "I have also inverted alphabets."

MR. THWAITES'S CYPHER.

Sir,—I feel much obliged to your correspondent "C." for the time and attention he has devoted to my challenge. (*Vide* Journal of September 15th.)

It would be ungenerous in me to do more than allude to the Number in question, and equally improper, (as regards the subject matter of my patent) to continue a controversy through any public channel until the objects of the patent are specified. Acknowledging the provoked attention of "C.," and his urbanity, I thank him—

"Quicquid sub terrâ est, in apricum proferet Ætas."

I beg to remain, yours faithfully,
JOHN H. B. THWAITES.

17 Park-street, Bristol, October 11th, 1854.

MR. THWAITES'S CYPHER.

22, Blenheim-street, Newcastle-on-Tyne,
October 8th, 1854.

Sir,—I beg to inform you that the ingenious method of secret writing which Mr Thwaites, of Bristol, has discovered, was *first* invented by Bishop Wilkins, more than half-a-century ago.

Two years since a gentleman in Cambridge lent me a work, of which the following is the title:—"The Mathematical and Philosophical Works of the Right Reverend John Wilkins, late Lord Bishop of Chester; to which is prefixed the Author's Life, and an Account of his Works. In Two Volumes. London: 1802."

The learned bishop gives the method of secret writing alluded to at page 29 of volume II. of the above-mentioned work; where he arranges ten alphabets to the key-word "Prudentia" just as Mr. Thwaites does to the word

"Telegraph." The only difference I can see between the two expositions of the method is this: the bishop allows us to proceed from one letter of the key-word to the next in three or four different ways, namely:—

I. At the beginning of a sentence.
II. At the beginning of a line.
III. At the beginning of a word.
IV. At every letter.

Whereas, Mr. Thwaites only admits of the last manner of proceeding. Mr. Thwaites justly observes that the method is capable of almost endless variety; I think, however, that the following deserves to be taken notice of: the alphabets may be arranged in three ways equally eligible, so as to spell the key-word, namely,—

The key word may be placed—

I. Horizontally (or vertically).
II. Slanting upwards.
III. Slanting downwards.

Thus, if *land* be the key-word, we may arrange in the three following ways.

I.

L	A	N	D
m	b	o	e
n	c	p	f
&c.,	&c.,	&c.,	&c.

II.

i	y	m	D
j	z	N	e
k	A	o	f
L	b	p	g

III.

a	L	a	l	a
b	m	A	m	b
c	n	b	N	c
d	o	c	o	D

In my opinion it is a better plan to pass from each alphabet to the next than it is to pass from the same fixed alphabet to others in succession.

Thus, taking the third arrangement of the alphabets to the key-word land it seems much easier to replace the word "blame" by m z m b p, than by n k z m p.

The insertion of this letter in the next number of the Journal of the society will greatly oblige,

Sir,
Your obedient servant.
J. B. KEARNEY, M.A.,
Curate of St. John's.

VOLUME II.

FROM NOVEMBER 11, 1853, TO NOVEMBER 10, 1854.

---

communication, we may consider the repeated keyword as a carrier wave on which the "random" waveform of the plaintext message is superimposed. Given this resulting waveform, which is the cryptogram or enciphered message, the problem is to deduce the periodicity of the carrier wave or key by investigation of whatever regularity that can be observed in the resulting waveform. Harmonic analysis is the splitting up of composite waveforms into their component waveforms. Clearly, it is this abstract notion that underlies Lindenfels' remark.

The double encipherment by two keys, as Babbage so rightly claims, is tantamount to the superposition of the corresponding two periodic waveforms prior to the addition of their resultant to the "random" waveform of the message. If this resultant is found, the question arises whether or not the two keys can be recovered. According to Maxwell, this is only possible if their corresponding waveforms are "conjugate". Mathematically, this implies, as we shall demonstrate in the APL terminal session, that the two periodicities are, what is known as, *relatively prime*. The meaning of this term is that, if the two periodicities are each written as a product of primes, they have no prime factor in common. But enough about the cryptographical content of the letters, let me now turn to their story.

Perhaps the word "story" is too presumptuous for what I now have to tell. Rather, what I intend to do, is to present the facts as I found them. This will enable

anyone to draw conclusions of his or her own, and perhaps even to do further research to dig up new facts which eventually might entangle the whole affair.

About Thwaites himself there is not much to say. [36]) We know that some time after 1854, he moved to another address in Bristol, and that his name disappeared from the city directory after 1865. Whether the last move was for good or more earthly is not clear. The manuscript index of the British Library, which includes the names of many correspondents of Babbage's, does not list him. [37])

In the published letters, Thwaites repeatedly refers to his pending patent. The printed patents record his provisional specification, entitled *"Apparatus to Facilitate Communication by Cypher"*, as *No. 1727, A.D. 1854*. [38]) The application is dated August 7th, 1854, and it was sealed on October 10th the same year. These dates agree with those published under the heading *"Patents Law Amendment Act, 1852"* in the Journal of the Society of Arts. The three-pages description states his full name, but apart from that we find no information supplementing his published letters. What is remarkable, however, is the fact that on the patent is printed in italics: *"Void by reason of the Patentee having neglected to file a Specification in pursuance of the conditions of the Letters Patent"*.

It might perhaps be expected that the correspondence which Babbage and Thwaites, respectively, had with the editor of the Journal of the Society of Arts, would answer the many puzzling questions such as, for example, why Babbage was writing anonymously. However, the letters which have been transcribed in figures 61 A to F, give only part of the total picture. [39]) Babbage's reference to *"Rees' Cyclopedia Att. Cypher"* in his letter of 2 Oct. 1854, may be expounded upon by the following remark in the anonymous article on *"Ciphers and Cipher-Writing"*, published 1871 under the signature *G.P.B.*: [21]) *"The best I have seen and full of curious information.* [A] *portion of the article ... is copied from Falconer's book* [published 1685]".

---

17 Park Street, Bristol
Aug. 28th 1854

My dear Sir,

Many thanks for your letter recd yesterday, and I trust you will allow me the opportunity of answering in the "Journal" any observations that may appear in its pages relative to my invention, and all communication that pass between us I shall hold sacred.

Believe me
Yours faithfully
John H.B. Thwaites

P.L.N. Foster, Esq. M.A.

Figure 61 A. From the correspondence of the Royal Society of Arts.
(Greater London Council, ref A/RSA, F. 4885)

17 Park St. Bristol
Sept. 5th 1854

Sir,

An able correspondent of your "Journal" date Sept. 1st 1854 signature C has afforded me much pleasure by his condemnation of my process of cyphering and decyphering, and also the apparatus connected therewith.

Professional engagements having accumulated during my short absence from home, rendered necessary for the provisional protection of that which I believe to be new in regard to the subject in question, must be my excuse for allowing this matter to pass without further comment until next week when I hope to be sufficiently free to dissiminate that which is new from the well known allusions of C of that which is old

I remain
Yours faithfully
John H. B. Thwaites

Figure 61 B. From the correspondence of the Royal Society of Arts. (Greater London Council, ref. A/RSA, F. 4987)

---

17 Park Street, Bristol
Sept. 11th, 1854

My dear Sir,

I shall indeed be much obliged if you will publish in your next "Journal" the enclosed letter in reply to C's communication of Sept 1st and I shall be still more pleased if you will let me know what you think of the matter – I myself feel so convinced that what I have brought forward is new that opposition does not at all affect me – Every one that I show it do say that they never saw described in any book or other manner a system similar to the one in question. I trust you will not think that I wish to make the "Journal" the medium of a controversy for my own ends, for nothing is so annoying to one as the semblance of a buff [?] – I only desire it to rest on its own merits, and if you see any thing in my letter that appears as such pray oblige me and erase it. Will you please cause to be forwarded to me fifty copies of the "Journal" in which my letter shall appear, and also let me know in what manner I can remit for them and the fifty I had a short time since

With many thanks for your courtesy and kindness,

Believe me
Yours very truly
John H. B. Thwaites

P.L.N. Foster, Esq., M.A

Figure 61 C. From the correspondence of the Royal Society of Arts. (Greater London Council, ref. A/RSA, F. 5042)

My dear Sir,

I send you some remarks on Mr. Thwaites' cypher. It seems to me to be the same in principle as one often alluded to.

Mr. T will find an account of it in Rees' Cyclopedia Att. Cypher.

I am, Yours truly
C. Babbage

2 Oc. 1854
Dorset St
Manch. Sq.

Figure 61 D. From the correspondence of the Royal Society of Arts. (Greater London Council, ref. A/RSA, F. 5001)

---

17 Park Street, Bristol
Oct. 11th 1854

My dear Sir,

I feel sure you will at once understand why I have no desire to continue the debate in the "Journal" at any rate at present: since now my specification is so full that I would not appear to borrow my points from C that I could embody in it – as an afterthought

C has unwittingly strengthened my hand but I will in the least degree take advantage of it

Will you oblige me by allowing the enclosed to appear in Friday's No – and with many thanks for your kindness.

Believe me
Yours very truly
John H. B. Thwaites

P.L.N. Foster, Esq., M.A

Figure 61 E. From the correspondence of the Royal Society of Arts. (Greater London Council, ref. A/RSA, F. 5249)

Dear Sir,

I am sorry that upon this occasion it is not in my power to aid the Society of Arts.

I have declined seeing the Diff. Engine of Mr. S [cheutz] *because at present it is a secret and a patent is being taken out. I have seen the inventors and was pleased with them*

I am informed that a Comm of the R. Soc. Prof. Stokes, Prof. Wheatstone & Prof. Willis have examined it and will report upon it.

I am myself too much occupied to admit of my helping any part on the request.

I am, Dear Sir
Yours faithfully
C. Babbage

Dorset St.
Manch. Sq.
10 Dec. 1854

Figure 61 F. From the correspondence of the Royal Society of Arts. (Greater London Council, ref. A/RSA, F. 1289)

In 1854, Babbage's youngest son, Major General Henry Prevost Babbage, was on leave from the Indian Army, staying with his father in London. In his privately printed *Memoirs and Correspondence*, published 1915, he recounts: [40])

> *"On 15 September I went to Hungerford Market (now the Charing Cross Railway Station) and by steamer to see Thames Tunnel. About this time a Mr. Thwaites had invented a cypher writing, which he submitted to the Society of Arts, with the hope of obtaining their medal. The Society referred the subject to my father, and asked his opinion.*
>
> *Thwaites proposed to use a keyword which he placed in line with a letter of the alphabet; this gave him as many alphabets as there were letters in the key-word, and he used them successively for the first, second and third letter of his writing and repeated this continually, thus if there happened to be seven letters in the key-word every seventh letter in the cypher would depend on the same alphabet. Having rendered his letter into cypher in this way he took a second key-word and treated the cypher-writing in the same manner.*
>
> *He was so convinced on the inscrutability of this system that he gave a couple of lines, together with the cypher produced by it, and challenged anyone to discover the process. My father & I puzzled over this for a day or two, when I made an example from two key-words of my own; they were two words each of four letters, or of four and six letters, I forget now. When I had done this I observed a certain symmetry in the position of the letters and I applied it to Thwaites's cypher, with the result that I found his key-word to be "two combined". I had used the known to reach the unknown, and my father was pleased. This was on the 25th September 1854. It was a blow to Mr. Thwaites; he had been beaten on his own ground. Instead of translating the writing into cypher twice over you might just as well do it once. With the keywords "two" and "combined" every twentyfourth letter of the writing would be translated into cypher with the same alphabet at one operation, instead of every third letter, and every eighth letter in two operations successively."*

Henry Prevost's statement on the medal, appears again to be only part of the story, for in his second letter, published in the Journal of the Society of Arts on September 15th, 1854, Thwaites remarks.

> *"In the first instance I made a free offer of my invention in a quarter where I had every reason to believe such a system was required; it was refused, and it was then I was induced to patent it for my own protection".*

Perhaps this *"quarter"* was the Foreign Ministry, for Babbage's cryptographical file in the British Library contains a puzzling draft of a letter which, signed F. Williamson, is transcribed in figure 62. Neither the name of Williamson, nor that

of Mr. Hammond mentioned in the draft, appears in the British Library index of manuscripts, which seems to list all of the significant correspondents of Babbage's in their collection. [41]) In view of Babbage's social position, it would not be surprising if the actual letter, or a copy of it, had been sent to him by the recipient, *"My Lord"*. But a rough draft?

Thwaites last letter, published in the Journal of the Society of Arts on October 13th, 1854, contains as his exit line part of a quotation from Horace, which in translation from Latin is: *"Time will bring to light whatever is hidden"*. Though, for our account, the missing part is perhaps even more appropriate: *" .. it will cover up and conceal what is now shining in splendour"*.

Life writes dramas no less intriguing than those of the playwright. Even an amusing twist is not outside the capability of fate. The last letter by J. B. Kearney, published in the Journal on October 20th, 1854, brings the clown on stage. For Babbage to read the entrance line about *"Bishop Wilkins, more than half-a-century ago"*, it must have been a great joke. Yet, also a little sad, as it closed the circle to the fond readings of his youth.

Front:

My Lord,

Having read a report of your speech in the Times
in which your L^dship pointed out
the danger that might arise from giving to the public the exact
words of a Telegraphic Dispatch written in cypher viz
that by placing "the cypher" on one side, and "the Decypher"
on the other, decypherers would readily discover the key,

I felt it my duty
from patriotic motives to inform your L^dship
that there can be no danger of this kind if the new
cypher recently invented by Mr Thw were em-
ployed by the Gov^mt Mr. T. has shown trium-
phantly that although he gives at length the trans-
lation and the cypher, as he has done in the Journal of

Back:

the Soc^y of Arts Sep. 1855 p. 733) yet it is impossible for
any one to read even his most simple cypher
"The most simple form is amply sufficient"
"for all practical purposes" vide Mr. Thwaites' letter
Mr Tw is perhaps the greatest decypher in Europe
and although I have the honour to be his friend
he is quite unacquainted with this letter Indeed
his modesty is such that I fear he
would be highly offended at it. If therefore you
should put Mr Hammond or any other gentleman
of the foreigh office in communication with him
I must entreat your L^d to conceal my name
from my friend whose address is
John H.B Thwaites, 17 Park St. Bristol

I am, Mylord
your ob^dt servant
F Williamson

Figure 62 The puzzling draft in Babbage's file. (Add.Ms. 37205, F. 139).

3.7 APL Terminal Session

By way of introduction, we briefly give a minimum of facts about the frequencies of occurrence of letters in the English language. Here, a remarkable fact, which we shall use later under the function name of *MINMAX*, is that the high-frequency letters: *ETAONIRSH* total 70% of all letters, and the low-frequency letters. *JKQXZ* only 1 to 2 %. We then proceed to the breaking of a monoalphabetic cipher, where the terminal session exactly documents what happened during a simulation of Babbage's approach. From there, using the Kasiski method followed by the min-max-approach, we break a polyalphabetic cipher, originally published by Thwaites as an advertisement, but later explained by him in his first letter to the Journal of the Society of Arts. We are then ready to consider Thwaites' as well as Babbage's challenge ciphers.

In either case, the plaintext is a quotation from *The Tempest*, act 1, scene 2, where Shakespeare lets Prospero, the right Duke of Milan, say to Ferdinand, son to the King of Naples:

> Pros. *Soft, sir! one word more*
> [aside] *They are both in either's powers; but this swift business*
> *I must uneasy make, lest too light winning*
> *Make the prize light.* [to Fer.] *One word more, I*
> *charge thee*
> *That thou attend me : thou dost here usurp*
> *The name thou owest not; and hast put thyself*
> *Upon this island as a spy, to win it*
> *From me, the lord on't*

Though, both ciphers drop the third line from the bottom.

In connection with Thwaites challenge, it may be of interest to mention that we introduce and apply the two well-known mathematical concepts of the *least common multiple* and the *greatest common divisor*. The approach for determining the prime factors, is based on Iverson's elegant APL formulation. [42]) An additional technique, implemented to cope with Babbage's challenge, is the so-called *symmetry of position* for reconstructing an alphabet. A standard method in cryptography, it is akin to the classical algorithm for picking a tree in a network, considering the network arcs one by one in the order in which they are listed. [43])


```
⍝       * * * LETTER FREQUENCIES * * *

⍝ A COUNT OF  DIGRAM FREQUENCIES  IN AN  ENGLISH
⍝ LITERARY TEXT, DISREGARDING THE WORD DIVISIONS
⍝ (SPACES) AND THUS CONSIDERING EVERY LETTER AS
⍝ THE FIRST OF A DIGRAM, IS GIVEN IN THE SQUARE
⍝ MATRIX   ENGLISH2  WITH ROW AND COLUMN INDICES
⍝ DEFINED BY THE NORMAL 26-LETTER ALPHABET   ABC

⍝ THIS MATRIX   ENGLISH2 , FORMS THE BODY OF THE
⍝ TABLE OF  FREQUENCIES OF ENGLISH DIGRAMS  SHOWN
⍝ ON A SEPARATE PAGE.

⍝ THE MORE IMPORTANT INFORMATION, WHICH CAN BE
⍝ DEDUCED FROM THE MATRIX  ENGLISH2 , WILL NOW
⍝ BE DISCUSSED

⍝ HOWEVER, BEFORE WE PROCEED, WE SHALL FIND IT
⍝ USEFUL TO DOCUMENT A PRINTING UTILITY FUNCTION
⍝ WHICH WAS ALSO USED EARLIER (SEE PAGE 189)

      CCPRINT
THE PRINTING WIDTH OF A NUMERICAL MATRIX  M  IS MINIMIZED
CONSIDERING THE COLUMNS INDIVIDUALLY AND LEAVING AT LEAST
ONE SPACE BETWEEN ADJACENT COLUMNS. THE WIDTH OBTAINED
DEPENDS UPON THE PRINTING PRECISION VALUE   ⎕PP

      ∇ PRINT[⎕] ∇
    ∇ Z←PRINT M
[1]  ASSUME →((2<⍴⍴M),2=⍴⍴M)/0,COLUMN
[2]   M←(1,⍴,M)⍴M
[3]  COLUMN →(0=¯1↑⍴M)/END
[4]   Z←(∨/   ≠⍕M[;⎕IO]),⍕M[;⎕IO]
[5]   Z←Z,' ',PRINT 0 1 ↓M
[6]   →0
[7]  END Z←((1↑⍴M),0)⍴''
    ∇

      ⍝ DIGRAM PROBABILITY

      ⍝ CLEARLY, THE TOTAL NUMBER OF LETTERS ON WHICH
      ⍝ THIS DIGRAM COUNT IS BASED, IS
      ⎕←TOTAL←+/+/ENGLISH2
10000
      ⍝ HENCE, ASSUMING  ABC  TO SPECIFY THE NORMAL
      ⍝ ALPHABET
      ⍴⎕←ABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ
26
      ⍝ THE PROBABILITY OF THE DIGRAM  ER , SAY, MAY BE
      ⍝ DETERMINED
      ENGLISH2[ABC⍳'E';ABC⍳'R']÷TOTAL
0.0154
      ⍝ SINCE DOUBLED LETTERS, LIKE  EE , OCCUR IN THE
      ⍝ MAIN DIAGONAL, SUCH PAIRS MAY BE FOUND
      (1 1⍉ENGLISH2)[ABC⍳'E']÷TOTAL
0.0039
      ⍝ WHILE REVERSALS SUCH AS  ER RE , BECAUSE OF THE
      ⍝ SYMMETRY IN POSITION ABOUT THE DIAGONAL, ARE
      1 1⍉ENGLISH2[ABC⍳'ER';ABC⍳⌽'ER']÷TOTAL
0.0154 0.0148
```

FREQUENCIES OF ENGLISH DIGRAMS


```
⍝           * * * MONOALPHABETIC SUBSTITUTION * * *

       ⍝ MONOGRAM FREQUENCIES

       ⍝ THE MONOGRAM OR SINGLE-LETTER FREQUENCIES ARE
       ⍝ PRODUCED TOTALLING THE ROWS (COLUMNS)
       PRINT 2 13⍴+/ENGLISH2
805 162 320 365 1231 228 161 514 718  10 52 403 225
719 794 229  20  603 659 959 310  93 203 20 188   9
       ⍝ SINCE, FOR REASONS OF CONSISTENCY, WE HAVE
       ^/(+/ENGLISH2)=+⌿ENGLISH2
1

       ⍝ GROUP PERCENTAGES

       ⍝ HIGH-FREQUENCY LETTERS:  ETAONIRSH
       (+/(+/ENGLISH2)[ABC⍳'ETAONIRSH'])×100÷TOTAL
70.02
       ⍝ LOW-FREQUENCY LETTERS:  JKQXZ
       (+/(+/ENGLISH2)[ABC⍳'JKQXZ'])×100÷TOTAL
1.11

       ⍝ VOWELS:  AEIOUY
       (+/(+/ENGLISH2)[ABC⍳'AEIOUY'])×100÷TOTAL
40.46

       ⍝ CONSONANTS:  LNRST
       (+/(+/ENGLISH2)[ABC⍳'LNRST'])×100÷TOTAL
33.43


⍝           * * * MONOALPHABETIC SUBSTITUTION * * *

       ⍝ BABBAGE'S PAPERS ON 'CYPHERS AND DECYPHERING' IN THE
       ⍝ BRITISH LIBRARY CONTAINS A NEWSPAPER CUTTING OF AN
       ⍝ ENCIPHERED ADVERTISEMENT IN THE TIMES, 21 SEPT 1854,
       ⍝ FOR WHICH NO SOLUTION IS GIVEN. (BL. ADD MSS  37205,
       ⍝ FOLIO 132)

       ⍝ THE FOLLOWING SESSION DOCUMENTS HOW IT WAS BROKEN,
       ⍝ SIMULATING BABBAGE'S APPROACH

       ⍝ THE ADVERTISEMENT RUNS AS FOLLOWS
       ⍴⎕←TMS540921
THIRTEEN
YLVZ ALHEZA AHVBGLY 'ZJSUO KLHXLYZ MHG'S BHF YZBF YHFL
-GU-FHXDY-EUGN-ZBFL-XLFEFILX-FLYUFLZBFLY-NUK-JEYSUO-
3 55

       ⍝ REWRITTEN WITHOUT PUNCTUATIONS, ETC.
       ⍴L←PUNCTUATION 0 1 1/TMS540921
9 110
       ⍴⎕←C←L REMOVE 0 1 1/TMS540921
YLVZALHEZAAHVBGLYZJSUOKLHXLYZMHGSBHFYZBEYHFLGUFHXDYEJGNZBFLXLFEFF
       ILXFLYUFLZBFLYNUKJEYSUO
96
```

THIRTEEN.—ylvz—alheza—ahv bgly'—zjsuo klhxlyz—mhg's—bhf—yzbf—yhfl—gu—fhxdy—eugn—zbfl—xlfefilx—fl yufl zbfly—nuk—jeysuo—

```
      ⍝ ASSUMING THAT THE LANGUAGE IS ENGLISH WE HAVE FOR A
      ⍝ PLAINTEXT THAT THE LETTERS
      ⍴⎕←ABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ
26
      ⍝ HAVE IN THIS ORDER THE EXPECTED FREQUENCY DISTRIBUTION
      ⍴⎕←FRQ←0.0001×+/ENGLISH2
0.0805 0.0162 0.032 0.0365 0.1231 0.0228 0.0161 0.0514
      0.0718 0.001 0.0052 0.0403 0.0225 0.0719 0.0794
      0.0229 0.002 0.0603 0.0659 0.0959 0.031 0.0093 0.0203
      0.002 0.0188 0.0009
26
      ⍝ CORRESPONDINGLY FOR THE CIPHER THE OBSERVED LETTER
      ⍝ FREQUENCY DISTRIBUTION IS
      ⍴⎕←DST←ABC FREQUENCY C
3 5 0 1 5 9 4 7 1 1 2 12 1 2 2 0 0 0 3 0 7 2 0 4 9 7
26
      ⍝ INVOKING THE FUNCTION
      DCFREQUENCY
THE RELATIVE FREQUENCY DISTRIBUTION  DST  OF
THE LETTERS IN A STRING OF  TXT  IS GIVEN IN
THE ORDER DETERMINED BY THE ALPHABET  ABC .

      ∇ FR[illegible]QUENCY[⎕] ∇
    ∇ DST←ABC FR[illegible]QUENCY TXT
[1]   DST←+/ABC∘.=,TXT
    ∇

      ⍝ APPLYING THE STATISTICAL 'PHI' TEST
      ⍴⎕←FRQ PHITEST DST
[illegible] 246 8[illegible]
3
      ⍝ WE SEE THAT THE INDEX OF COINCIDENCE FOR THE CIPHER
      ⍝ I.E. 243 , IS FAR CLOSER TO THE CORRESPONDING INDEX
      ⍝ [illegible]46.84 FOR A PLAINTEXT THAN TO THE INDEX 14[illegible].8[illegible]
      ⍝ FOR A RANDOM TEXT

      ⍝ SINCE FURTHER THE OBSERVED DISTRIBUTION  DST
      ⍝ DOES NOT MATCH THE CONVENTIONAL ALPHABET  ABC , AS
      ⍝ WOULD BE OBTAINED BY A TRANSPOSITION CIPHER, WE
      ⍝ CONCLUDE THAT THE CIPHER IS A MONOALPHABETIC OR
      ⍝ SIMPLE SUBSTITUTION.


      ⍝ THE CIPHER ALPHABET

      ⍝ A CONVENIENT AID NOW, IS THE FUNCTION
      DCREORDER
RESULT  R  IS A COLUMN MATRIX LISTING, IN ORDER
OF DECREASING RELATIVE FREQUENCY, THE ALPHABET
 XYZ  AND ITS ASSOCIATED DISTRIBUTION  DST

      ∇ REORDER[⎕] ∇
    ∇ R←XYZ REORDER DST;A[illegible]
[1]  ASSUME ∧((⍴XYZ)≠⍴DST)/0
[2]   [illegible]
[3]   R←[illegible]⍴XYZ [illegible]XYZ[A[illegible]][illegible]DST[A[illegible]][illegible] 0
    ∇
```



```
      ⍝ THUS, REORDERING THE CIPHER LETTERS IN DECREASING ORDER
      ⍝ OF OCCURRENCE AND COMPARING THIS WITH THE CORRESPONDINGLY
      ⍝ REORDERED AND RESCALED PLAINTEXT FREQUENCIES WE FIND
      ⍴⎕←(ABC REORDER FRQ×⍴C),XYZ←ABC REORDER DST
E   10.71     L 12
T    8.3433   F  9
A    7.0035   [illegible]  9
O    6.9078   H  7
N    6.2553   U  7
I    6.2466   Z  7
[illegible]    5.7335   B  5
R    [illegible]      F  [illegible]
[illegible]    [illegible]      G  4
[illegible]    3.5061   X  4
     3[illegible]         A  3
     2.784    [illegible]  3
[illegible]    2.677    K  2
P    1.9723   N
F    1.9836   O
M    1.9575   V  [illegible]
W    1.7661   D
[illegible]    1.635[illegible]   I  [illegible]
G    1.4094   J  [illegible]
[illegible]    1.4007   M  1
[illegible]    [illegible]      [illegible]
[illegible]    [illegible]      P  0
[illegible]    0.[illegible]      Q  0
[illegible]    [illegible]      R  0
[illegible]    0.087    T  0
[illegible]    0.0703   W  0
[illegible]
      ⍝ THIS REVEALS THAT THE ONLY LETTERS APPEARING IN THE
      ⍝ CRYPTOGRAM ARE
      [illegible]
    [illegible]
1[illegible]
      ⍝ LEAVING OUT THE LETTERS
      [illegible]
[illegible]

      ⍝ HENCE, THE CIPHER ALPHABET  XYZ  IS, LISTING ONLY THE
      ⍝ USED LETTERS IN DECREASING FREQUENCY OF OCCURRENCE
      [illegible]
 [illegible]DFGXAS[illegible]NOVDI[illegible]M


      ⍝ STANDARD TESTS

      ⍝ CERTAIN STANDARD TESTS BASED ON CLASSICAL ALPHABETS
      ⍝ SHOULD INTRODUCE THE ANALYSIS OF A CRYPTOGRAM MADE
      ⍝ BY SIMPLE OR MONOALPHABETIC SUBSTITUTION

      ⍝ ESSENTIALLY THREE TYPES OF ALPHABETS ARE TESTED,
      ⍝ NAMELY A CAESAR OR SHIFTED ALPHABET, A REVERSED
      ⍝ OR SOCALLED INVERTED ALPHABET, AND A RECIPROCAL
      ⍝ ALPHABET.
```

```
      ⍝ TO ILLUSTRATE, CONSIDER THE CRYPTOGRAM IN THE TIMES,
      ⍝ 21 SEPT 1854, IN ITS  CLEANED  FORM
      ρ⎕←C
YLVZALHEZAAHVBGLYZUSJOKLHXLYZMHGSBHFYZBEYHFLGUFHXDYEUGNZBFLXLFEF
ILXFLYJFLZBFLYNUKJEYSJO
87
      ⍝ A CONVENIENT FRACTION MAY BE
      ρ⎕←V←22↑C
YLVZALHEZAAHVBGLYZUSJO
22

      ⍝ CAESAR OR SHIFTED ALPHABET DERIVES FROM
      ρ⎕←ABC
ABCDEFGHIJKLMNOPQRSTUVWXYZ
26
      ⍝ HENCE  V  IS SHIFTED AS USUAL

      ⍝ REVERSED OR INVERTED ALPHABET
      ρ⎕←⌽ABC
ZYXWVUTSRQPONMLKJIHGFEDCBA
26
      ⍝ HENCE WE MUST SHIFT THE FRACTION
      ρ⎕←ABC[⌽ABC⍳V]
BOEAZOSVAZZ9EYTOBAFHFL
22

      ⍝ RECIPROCAL ALPHABET
      ρ⎕←XYZ←(13ρ 13↑ABC) 13↑ABC
NOPQRSTUVWXYZ
ABCDEFGHIJKLM
2 13
      ⍝ SO THAT WE MUST SHIFT THE FRACTION
      ρ⎕←ABC[(,XYZ)⍳V]
LYIMNYURMNNUIOTYLMNFHB
22

      ⍝ IN ALL THREE CASES, HOWEVER, SUBMITTING THESE
      ⍝ FRACTIONS TO THE FUNCTION  SHIFT , NO RESULT
      ⍝ OF INTEREST IS OBTAINED

      ⍝ WE CONCLUDE, THEREFORE, THAT THE SUBSTITUTION IS
      ⍝ BASED ON AN ALPHABET PERMUTED IN A DIFFERENT WAY

      ⍝ NGRAM SEARCH

      ⍝ TO FIND REPEATED NGRAMS, WE INTRODUCE THE FUNCTION
      REPEAT
ASSUMING LEFT ARGUMENT  MN  TO BE A 2-ELEMENT NUMERICAL
VECTOR   MN←MIN,N  (BOTH ≥1), THE RIGHT ARGUMENT  TXT
(CONCEIVED AS THE CHARACTER STRING   ,TXT ) IS SEARCHED
FOR ALL  N -GRAMS REPEATED AT LEAST  MIN  TIMES. RESULT
 R  IS A CHARACTER  COLUMN  MATRIX OF THESE  N -GRAMS
ORDERED AS TO THEIR LISTED FREQUENCY OF OCCURRENCE.
```



```
      ∇ REPEAT[⎕]∇
    ∇ R←MN REPEAT TXT;MIN;N
[1]   ⍝ ASSUME  ^/1≤MN ^  ∧/1≥⍴⍴TXT) 0
[2]   ARG MIN←1⌈1↑,MN
[3]    N←1⌈ 1↑ MN
[4]   MAIN TXT←⍉ 0 1 N↓((⍳N)∘.+⍳(N ρ TXT ρ,TXT
[5]    R←+/ ∧TXT∧  ⍉TXT
[6]    N←⍒R
[7]    R←(R[N] MIN)/TXT[N ],(R[N] ),0
    ∇

      ⍝ TWO AND HIGHER ORDER NGRAMS

      ⍝ DIGRAMS OCCURRING AT LEAST TWICE IN THE CIPHER
      ρ⎕←2 REPEAT C

      ⍝ TRIGRAMS OCCURRING AT LEAST TWICE
      ρ⎕←2 3 REPEAT C

      ⍝ TETRAGRAMS OCCURRING AT LEAST TWICE
      ρ⎕←2 4 REPEAT C

      ⍝ HIGHER ORDER NGRAMS DO NOT OCCUR IN THE CIPHER
      ρ⎕←2 5 REPEAT C

      ⍝ BY VISUAL INSPECTION

      ⍝ IT IS NOT KNOWN WHETHER THE WORD DIVISIONS ARE CORRECT

      ⍝ HOWEVER, IF THEY ARE THE CIPHER CONTAINS THE FOLLOWING
      ⍝ PATTERN WORDS AS DETERMINED BY VISUAL INSPECTION
      ⍝ ALHEZA
6
```

```
      ⍴ ZUSUO
5
      ⍴ KLHXLYZ
7
      ⍴'XLFEFILX
8
      ⍴ FLYUFLZHFLY
11

      ⍝ NOTE THAT THE LAST MENTIONED PATTERN WORD CONTAINS THE
      ⍝ REPEATED TETRAGRAM   ZHFL ,  APPEARING ALSO AS AN
      ⍝ INDEPENDENT WORD

      ⍝ SORTING THE WORDS IN INCREASING ORDER ACCORDING TO
      ⍝ WORD LENGTH WE FIND BY INSPECTION THE FOLLOWING
      ⍝ CLASSES

      ⍴⎕←W2
GO
1 2
      ⍴⎕←W3
BHF
NJK
[illegible] 3
      ⍴⎕←W4
FLRN
ZHFL
YH F
YLVZ
YZHE
5 [illegible]
      ⍴⎕←W5
FHXDY
INHG S
ZUSUO
3 6
      ⍴⎕←W6
ALHEZA
JEYSUO
2 6
      ⍴⎕←W7
AHVBOLY'
KLHXLYZ
2 8
      ⍴⎕←W8
XLFEFILX
1 8
      ⍴⎕←W11
FLYUFLZHFLY
1 11


      ⍝ THE AVERAGE WORD LENGTH IS
      [illegible]
5.2941
      ⍝ WHICH SHOULD BE COMPARED WITH A PLAINTEXT AVERAGE OF
      ⍝ '4.5' LETTERS PER WORD
```



```
      ⍝ A CRYPTOGRAPHIC SKETCHPAD

      ⍝ BABBAGE, WE RECALL, DEMANDED THAT THE LINES OF THE
      ⍝ CRYPTOGRAM OF CAPTAIN CHILDE WERE SPACED APART IN
      ⍝ ORDER THAT HE COULD ENTER HIS TRIAL SOLUTIONS. A
      ⍝ FUNCTION PROVIDING THIS FACILITY, MAY BE
      CCINTERPRET
INTERACTIVE SKETCHPAD FOR PRODUCING A PLAINTEXT
SOLUTION  P  FROM A CRYPTOGRAM  C   MONADIC FORM
(I.E., LEFT ARGUMENT  TRY  IS AN EMPTY VECTOR)
STARTS WITH A BLANK  P , WHEREAS THE DYADIC FORM
BEGINS WITH A PREVIOUS SOLUTION  TRY , REQUESTED
INPUTS   CIPHER   AND   PLAIN ,  PROVIDING THE
CHARACTER TRANSFORMATION FROM 'C' TO  P , MUST
CONFORM IN SIZE.  OTHERWISE THE INPUT REQUEST
IS REPEATED
        EXIT BY CARRIER RETURN

      ∇ INTERPRET [⎕] ∇
    ∇ [illegible] OLD NEW L AUX
[1]  [illegible]
[2]  [illegible]
[3]  [illegible]
[4]  DYADIC P←(⍴,C)⍴TRY
       PRINT
[5]  NXT [illegible]
[6]  [illegible]
[8]  OUT ←(0=⍴OLD←8↑B)/0
[9]  [illegible]
[10]  NEW←B↓⍞
[11]  [illegible]
[12] REPLACE L←OLD∘.  [illegible]
[13]  AUX←(ι⍴OLD)+.×L
[14]  [illegible]
[15]  P←(⍴C)⍴(NEW,,P)[AUX]
[16] PRINT (⎕IO← 1 8 2)⍉(2,⍴C)⍴(,C),,P
[17]  →NXT
    ∇

      ⍝ THE FUNCTION IS EQUALLY USEFUL FOR ANALYSIS OF THE
      ⍝ CONSONANT/VOWEL PATTERN AND FOR THE GUESSING OF
      ⍝ PROBABLE WORDS

      ⍝ THE PROBABLE WORD METHOD

      ⍝ THE BASIC APPROACH USED BY BABBAGE TO SOLVE THE
      ⍝ VARIOUS CRYPTOGRAMS IN THE SOCALLED  AGONY COLUMNS
      ⍝ OF THE NEWSPAPERS, SEEMS TO BE THE GUESSING OF A
      ⍝ WORD

      ⍝ INVESTIGATION OF THE DIFFERENT  ADS  SOLVED BY
      ⍝ BABBAGE REVEALS, APART FROM THE USUAL SHORT WORDS
      ⍝ OF 2-4 LETTERS, A RICH REPETITION OF WORDS LIKE
      ⍝ 'DEAR, DEAREST, LOVE, HEALTH, ADIEU, RECEIVED,
      ⍝ ANSWER, PRAYER, GOD-BLESS-YOU , ETC.
```

```
* TO ILLUSTRATE THE METHOD CONSIDER THE CIPHER IN
* THE TIMES, 21 SEPT 1854
ρ□+TMS540921
THIRTEEN.-
YLVZ-ALHEZA-AHVBGLY'-ZUSUO-KLHXLYZ-MHG S-BHF-YZBE'-YHFL
 GU FHXDY-EUGN-ZBFL-XLFEFILX-FLYUFLZBFLY-NUK JEYSUO
3 55

* HAVING PERFORMED THE STANDARD STATISTICAL TESTS
* WE FOUND THAT CIPHER LETTER  L  IS PROBABLY
* PLAIN TEXT LETTER 'E', ASSUMING CORRECT WORD
* DIVISIONS, WE THEN PROCEED AS FOLLOWS
NOW←''INTERPRET  0 1 1/TMS540921
YLVZ ALHEZA AHVBGLY ZUSUO KLHX YZ MHG S BHF YZBE  YHFL
 GU FHXDY EUGN ZBFL XLFEFILX FLYUFLZBFLY NUK JEYSUO

CIPHER  - L
PLAIN   - E
YLVZ ALHEZA AHVBGLY'-ZUSUO KLHXLYZ MHG S BHF-YZBE  YHFL
 E  - E        E -      - E  E          -  -          E

-GU-FHXDY-EUGN-ZBFL-XLFEFILX-FLYUFLZBFLY-NUK-JEYSUO-
-  -     -    -    E- E    E - E   E   E-   -      -

      WORD  KLHXLYZ  HAS THE PATTERN OF  DEAREST


CIPHER  KLHKYZ
PLAIN   DEARST
YLVZ-ALHEZA AHVBGLY  ZUSUO KLHXLYZ MHG S BHF YZBE  Y [illegible]
SE T- EA T - A   ES -T    -DEAREST- A ' - A -ST  '-SA E

 GU FHXDY EUGN ZBFL XLFEFILX FLYUFLZBFLY NUK  EYS [illegible]
-  - AR S-    -T  E RE    ER- ES  ET  ES-  D-  S


      WORD  ALHEZA  HAS NOW THE PATTERN OF 'HEALTH


CIPHER  AE
PLAIN   HL
YLVZ-ALHEZA-AHVBGLY'-ZUSUO-KLHXLYZ-MHG S-BHF-YZBE'-YHFL
BE T-HEALTH-HA   ES'-T    -DEAREST- A ' - A -ST L'-SA E

-GU-FHXDY-EUGN ZBFL-XLFEFILX-FLYUFLZBFLY-NUK-JEYSUO-
-  - AR S-L   -T  E-RE L  ER- ES  ET  ES-  D- LS   -

      NOTICING THAT THE PAIR  LE  IS RECIPROCAL IN
      THIS TRANSFORMATION, WE GUESS THAT THE WORD
       KLFEFILX  SHOULD HAVE BEEN  REMEMBER  IF NOT
      FOR AN ENCIPHERMENT ERROR MIXING  E  AND  L
```



```
CIPHER  FI
PLAIN   ME
 [illegible] AHVBGLY  ZUSUO KLHX [illegible]  MHG S BHF YZBE  YHFL
SE I-HEALTH-HA   ES -T      DEAREST- A ' - AM-ST L'-SAME

 [illegible] FHXDY [illegible] ZBFL XLFEFILX FLYUFLZBFLY NUK-JEYSUO
-  -MAR S-L   -T ME-REM MBER-MES MET MES-  D- LS   -

      THE TWO WORDS  ZBFL  AND  FLYUFLZBFLY  ARE CLEARLY
      THREE, NAMELY,  TIME ,  ME , AND  SOMETIMES

CIPHER  BL
PLAIN   IO
YLVZ ALHEZA AHVBGLY'-ZUSUO KLHXLYZ MHG S BHF-YZBE'-YHFL
SE I HEALTH HA I ES' TO D  DEAREST - A ' -IAM-STIL'-SAME

 GU FHXDY EUGN ZBFL XLFEFILX FLYUFLZBFLY-NUK-JEYSUO-
  O-MAR S LO  -TIME REMEMBER MESOMETIMES- OD- LS O -

      THERE CAN NOW BE NO DOUBT THAT THE CIPHER ALPHABET
       XYZ  IS RECIPROCAL, SO WE INTRODUCE ALL KNOWN PAIRS

CIPHER  DRSTHY
PLAIN   KXYZFI
 [illegible] KLHXLYZ MHG S [illegible] YHFL
SE T HEALTH HA I ES'-TOYOU-DEAREST-FA 'Y-IAM-STIL'-SAME

 [illegible] NUK JEYSUO-
  O MARKS LO  -TIME REMEMBER MESOMETIMES- OD- LSYOU-

      EVIDENTLY THE WORDS  GU  AND  EUGN  MUST BE
       NO  AND  LONG  RESPECTIVELY

CIPHER  NG
PLAIN   GN
 [illegible] AHVBGLY  ZUSUO KLHXLYZ MHG S BHF YZBE  YHFL
SE T HEALTH HA INES'-TOYOU DEAREST FAN Y-IAM-STIL'-SAME

 [illegible] ZBFL [illegible] ZBFLY NUK JEYSUO
NO-MARKS LONG TIME REMEMBER MESOMETIMES GOD- LSYOU-

      FROM THE WORDS  YLVZ  AND  AHVBGLY'  IT IS OBVIOUS
      THAT, DISREGARDING MISSPELLINGS,  V" MUST BE  P

CIPHER  V
PLAIN   P
YLVZ ALHEZA AHVBGLY -ZUSUO KLHXLYZ-MHG S-BHF-YZBE'-YHFL
 [illegible] DEAREST FAN Y IAM STIL  SAME

 [illegible] NUK  JEYSUO
 [illegible] MBER MESOMETIMES GOD  LSYOU


      FINALLY,  J  AND  I  MUST BOTH BE  B  SO THAT THE
      TWO WORDS  NUK JEYSUO  READS  GOD BLESS YOU
```

```
IPHER
PLAIN    B
YLVZ ALHEZA ANVHGLY'-ZUSJO-KLHXLYZ-MHG S-BHF YZBE -YHFL
[illegible]

[illegible]
NO MARKS LONG TIME REM MBER MESOMETIMES GOD BLSYDI
```

* REMARKS ON THE SOLUTION

* THUS, WE HAVE FOUND THAT THE TRANSLATION OF THE
* CIPHER IN THE TIMES, 21 SEPT 1854

```
TMS'4'921
THIRTEEN
YLVZ-ALHEZA-ANVHGLY -ZJSJO-KLHXLYZ MHG S-BHF-YZBE'-YHFL
[illegible]
```

* SHOULD READ AS FOLLOWS

```
TMS'540? [illegible] [1]N)W
THIRTEEN
SEPT HEALTH-HAPINES -TOYOU DEAREST FAN Y-IAM STIL' SAME
NO MARKS LONG TIME-REMEMBER MESOMETIMES GOD B[illegible]
```

* CONTAINING ONE ENCIPHERMENT ERROR

* THE RECIPROCAL CIPHER ALPHABET XYZ USED TO
* PRODUCE THIS CIPHER, IS CLEARLY OF ONLY 24
* LETTERS, CONSIDERING I AND J IDENTICAL AND
* C AND K IDENTICAL

* THAT IS, THE CIPHER ALPHABET HAS BEEN PRODUCED
* FROM THE CONVENTIONAL ALPHABET AS FOLLOWS

```
    ⍝□←XYZ←2 2 6⍴(⍴ABC)~CJ )/ABC
ABDEFG
HIKLMN

OPQRST
UVWXYZ
2 2 6
    ⍝□←XY/←⍝XYZ[1 ;] XYZ[2 ;]
HIK MNUVWXY
ABDEFGOPQRST
2 12
    [illegible]
ABCEFGHIKLMNOPQRSTUVWXYZ
HIKLMNABDEFGUVWXYZOPQRST
2 24
```

THIRTEENTH.—Mhggs—Nuk—Ielyy—suo [illegible]—
Gs—fhxd—gsq—[illegible]

* TWO YEARS LATER

* APPARENTLY THE CORRESPONDANCE CONTINUED FOR BABBAGE
* SAVED YET AN UNDECIPHERED CLIPPING FROM THE TIMES,
* 13 SEPT 1856, RUNNING AS FOLLOWS (BL. ADD MS. 37205,
* F 192)

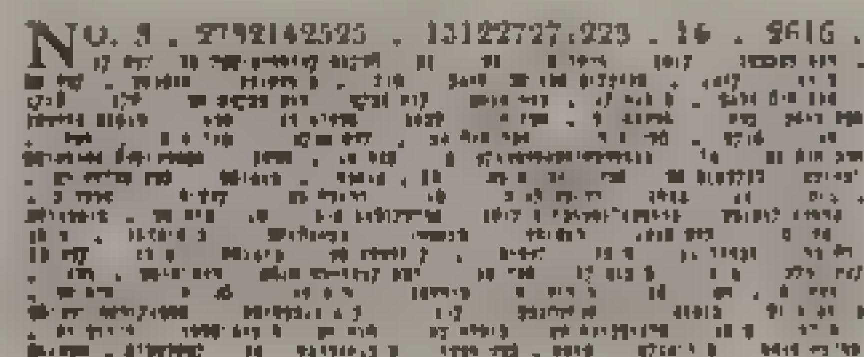
```
    ⍝□←TMS'60913
THIRTEENTH, — MHGGS-NUK IELYY-SUO-SJOX-GL-FHXD GLQ
          [illegible]
2 50
```

* A CHALLENGE

* ANOTHER CIPHER OF THE SAME KIND, THOUGH WITH A NUMERICAL
* RATHER THAN A CHARACTER REPRESENTATION OF THE PLAINTEXT
* LETTERS, APPEARED IN THE MORNING CRONICLE, 22 OCT 1833
* (BL. ADD MS. 37205, F.23). IT WAS PART OF A LONGER
* CORRESPONDANCE OF WHICH BABBAGE SAVED THE TRANSLATIONS
* IN HIS FILE

* WITH PRINTING AND ENCIPHERMENT ERRORS, IT RAN AS
* FOLLOWS IN THE NEWSPAPER

```
    ⍝□←MC331022
  NO 5.   2732142525 , 131227271223 . 14  . 2616    171627
101726122325271017 26 31 22 311025 .1017 .1223231623.221827
201618 32102912 .1716 .2416172014261217 2412.1417 1512.1716
1716.231027321223.27321017.20161823.17101512 ,253216181326
[illegible]
26121226 . 1628  15141712 ,27321027 .2416181326 , 13121026
2716 . 10 , 26142524162912 2320  , 1628  , 161823
1417271223241618232512 . 14 . 3116181326 . 231027321223
261412 .103010 . 10 . 32181726231226 , 2612102732 , 221827
313220 131227.25182432 10 3123122432.1025 14 1015.30142912
201618 10 15161512172725 1017121025201712 2525 221017142532
15231615 .20161823 .102012 201623 .12291223 101726 .131227
[illegible]
20161823 ,2610183032271223 101726 ,27121313,1512 ,27321027
201618 . 101726 .101313 . 102312 .31121313  24  28  321025
2312271823171226 . 2618221317417 . 1417 . 22162620 . 141015
2110142712 . 31121313 . 1026141218 . 201618 . 32102912
[illegible]
12291223 . 2212 . 27141313 . 2612102732
19 50
```


NO. 5 . 2732142525 . 131227271223 . 14 . 2616 .
[illegible]

```
⍝         * * * THE AUTOKEY CIPHER * * *

⍝ THE  CIPHER NO. 1 , COMPOSED BY DR. FITTON S SISTER,
⍝ MRS. JAMES, ACCORDING TO A MISTAKEN ENUNCIATION OF
⍝ THE  AUTOKEY  LAW BY GILBERT AND BABBAGE, IS FILED
⍝ AMONG THE LATTER S CRYPTOGRAPHIC MANUSCRIPTS IN THE
⍝ BRITISH LIBRARY (ADD. MS. 37205, FF. 268-269).

⍝ BABBAGE S SOLUTION TO THE FIRST LINE IS
⍝  THE QUESTION TO WHAT PRACTICAL END AND ADVANTAGE..

⍝ FOLLOWING BABBAGE S DESCRIPTION AS QUOTED FROM HIS
⍝  PASSAGES , THE READER MIGHT FIND IT OF INTEREST TO
⍝ WRITE A FUNCTION THAT PRODUCES  CIPHER NO. 1 . IF IT
⍝ IS DONE CORRECTLY IT SHOULD MATCH THIS TRANSCRIPTION
⍝ FROM HIS MANUSCRIPTS

      CRPT268
HDE  AIKWULRK  XF FQYJ  ULDHJCDAZ  TIJ FWV TYLDYJFPD OD YEEB
EOSAORZWWK XVOL7  LV HJY MUNDS  PGM  UJUHBYGRFED PDGJINPOHLU
QFX  CAJUX  BACIRBGEO  FXI GTN PVG  AJKI.  OVW WFSKCE.  XW S
NBOQMPZA  PDTIM  LBBHSZ  TIPNZ,  INF VXIK  GWFCGKTOIZXFW  GN
IBZDBAWDCE XRA  AIZJFJFH  KIVXENBAH AFDERP,  DNO SAZSKQ FNDE
JOREYKX  R  PBYIK SB  UOMKPHHAWDV.  AS BRBYI ZWSP SDPGC UM C
XFOTT VGL GQGGVNOZTNUYT  KPDLVNSA WF QGA  GXVVNMCFRLGQ URVVA
LODHA HV XDEWHA HOEW  XIUG AIIN  RRBFCUITDYW,  UISIABVVTOITB
NT DHUB QM VH QIY  EOV FRKH AVX  GCDPRQ  FJUJNOECE KJYJL WZT
ZMBZRFBR LI ZWW TZCQTJQCZI GVW EYHHS DRBYYDRP NG ERFLK LXDLQ
LDEEBR FB FDDNFYJNCXV.  TIJ YUHKMPF CA HOE SJOULB BL QM QLH.
DE WALBO AIXVEI BTGMIK XYYI QA D SGDQGKMGVM CZS ZXIFGB EOPKC
FX KLRPD HOO.  HHCUHN  LBRJXVEFNT  GGRQJJ HHWSYYJD  LQB YUML
UHSECT ACD  TIZTBTZRGSWD AIXJZXKW.  SNF LAKWLDYJQW JJUYQRFWT
KT.S DTH AVBF NRNVPEI


⍝      * * * THWAITES' ADVERTISEMENT * * *

⍝ KASISKI ANALYSIS AND STATISTICAL  MINMAX  SOLUTION
⍝ OF THWAITES  ADVERTISEMENT IN THE TIMES, 21 JULY
⍝ 1854, QUOTED IN HIS FIRST LETTER IN THE JOURNAL OF
⍝ THE SOCIETY OF ARTS. THE NEWSPAPER CUTTING FROM THE
⍝ TIMES IS KEPT AMONG BABBAGE S PAPERS (BL. ADD MSS
⍝ 37205, F.126)

      ⍴⎕←CRPT126
GZZES, GV, TNSRXWVFOO, LXWV, QBOJZ
FXHFJBX, GXNOZEO, RBXDU, SO, FRTGYBMF
XY, DUDB, SLJP, TAUB, VJPTQRSIW, JTZ
SD, EJPLMOFF, ZUGQSCG  —  VBBV.
4 38
      ⍴C←PUNCTUATION CRPT126
9 152
      ⍴C←L REMOVE CRPT126
102
```



```
⍝      * * * THWAITES  ADVERTISEMENT * * *

      ⍝ REPEATED NGRAMS

      2 3 REPEAT C
XWV 2

      2 REPEAT C
ZE 2
GV 2
XW 2
WV 2
LO 2
FX 2
BX 2
DL 2
OF 2
OB 2
PT 2
DV 2
 P 1

      ⍝ TOOLS FOR DETERMINATION OF PERIODICITY

      ⍝ TO DETERMINE THE PERIODICITY OF THE KEY, THREE TOOLS
      ⍝ ARE NEEDED, THAT IS, WE MUST FIND THE POSITIONS OF THE
      ⍝ REPEATED NGRAMS, THE DISTANCES BETWEEN THE REPETITIONS,
      ⍝ AND THE PRIME FACTORIZATION OF THESE DISTANCES.

      ⍝ THE FOLLOWING THREE FUNCTIONS ARE DESIGNED TO DEAL EACH
      ⍝ WITH ONE OF THESE PROBLEMS, THUS.

      CCIN
A STRING OF  TXT  IS SEARCHED FOR THE INITIAL
INDEX OF EACH OCCURRENCE OF THE NGRAM  NGR .

      ∇ IN[⎕] ∇
    ∇ I←NGR IN TXT
[1]    I← ... NGR  ⎕IO ... TXT)/⍳⍴TXT
    ∇

      CCDIF
THE ABSOLUTE VALUES  R  OF THE FIRST DIFFERENCE
OF A NUMERIC VECTOR  V .

      ∇ DIF[⎕] ∇
    ∇ R←DIF V
[1]    R←|1↓V-¯1↓V
    ∇
```


GZZES, gv, tnsrxwvfoo, lxwv, qbojz, fxbfjbx,
VBBV, July 20th, 1854.

```
        FP⍙MFFA T H
RESULT  R  IS A MATRIX OF PRIME FACTORS OF THE
VECTOR (SCALAR)  V  OF NON NEGATIVE INTEGERS. IN
PARTICULAR, CORRESPONDING TO THE PRIMES IN THE
UPPER ROW OF  R , THE EXPONENTS OF EACH INTEGER
ARE GIVEN ROWWISE IN THE REMAINDER ROWS ORDERED
ACCORDING TO  V .

      ∇ PRIMEFACTOR[⎕] ∇
    ∇ R←PRIMEFACTOR V;⎕IO N F P
[1]   [illegible]
[2]  DIVISIBILITY N←⌈/V
[3]   R←0=(⍳N)∘.|⍳N
[4]   F←R[,V]
[5]  PRIMES P←(∨⌿F)∧2=+⌿R)/⍳N
[6]  FACTORS F←F×(⍴F)⍴⍳N
[7]   [illegible]
[8]   R←P[1]⍪+/R×(⍴R)⍴1=+/R
    ∇

      ⍝ [illegible] KEY PERIOD

      ⍝ THE TRIGRAM  XWV
       XWV  IN C
 [illegible]
        [illegible]
[illegible]
      ⍝ [illegible] BEING A PRIME, MAY BE THE PERIOD

      ⍝ VARIOUS DIGRAMS
       YE' IN C
 [illegible]
      DIF 3 38
[illegible]
      PRIMEFACTOR 35

 [illegible]
       GV' IN C
6 98
      DIF 6 98
92
      PRIMEFACTOR 92
 2 23
 2  1

      ⍝ DIGRAMS  XW  AND  WV  ARE PARTS OF TRIGRAM
      ⍝  XWV  AND ARE HENCE OF A PERIOD OF 7

       LO  IN C
16 59
      DIF 16 59
43
      PRIMEFACTOR 43
 43
  1
```



```
       FX  IN C
27 55
      DIF 27 55
28
      PRIMEFACTOR 28
 2 7
 2 1

      ⍝ IT THUS APPEARS THAT WE HAVE A KEY LENGTH OF 7

      ⍝ TOOLS FOR A KASISKI SOLUTION

      ⍝ ASSUMING THAT NO CIPHER ALPHABET HAS BEEN USED, WE MAY
      ⍝ ATTEMPT A STATISTICAL SOLUTION OF THE KASISKI MATRIX.

      ⍝ FOR THIS PURPOSE, WE NEED THE FOLLOWING THREE FUNCTIONS
      ⍝ IN ADDITION TO THE FUNCTION   SHIFT   (SEE PAGE 56)

      ⍝⍝KASISKI
RESHAPING OF A STRING OF TEXT  V  (PADDED WITH
BLANKS INSTEAD OF REPEATING THE ELEMENTS) INTO
A MATRIX  M ,  WHOSE NUMBER OF COLUMNS  N  IS
THE PUTATIVE PERIOD OF THE KEYWORD

      ∇ KASISKI[⎕] ∇
    ∇ M←N KASISKI V
[1]   M← [illegible]
    ∇

      ⍝⍝KMETHOD
ASSUMING LEFT ARGUMENT  M  TO BE A KASISKI MATRIX
THE RESULT  R  IS PRODUCED SUBSTITUTING EACH COLUMN
BY ITS GENERATRIX OF THE LARGEST DIFFERENCE BETWEEN
THE TWO COUNTS OF HIGH AND LOW FREQUENCY LETTERS
RESPECTIVELY
      ASSUMED AVAILABLE   ALPHABET   ABC
      AND  FUNCTIONS   SHIFT   AND   MINMAX

      ∇ KMETHOD[⎕] ∇
    ∇ R←KMETHOD M,N,AUX
[1]   [illegible]
[2]   R←(⍴M)⍴' '
[3]  NXT AUX←~M[;N]∊' '
[4]   [illegible]
[5]   N←N+1
[6]   [illegible] NXT
    ∇

      ⍝⍝MINMAX
A CHARACTER VECTOR  TXT  IS SHIFTED THROUGH THE
ALPHABET  ABC ,  TAKING FOR EACH GENERATRIX A
FREQUENCY COUNT OF THE TWO GROUPS  MAX  AND  MIN
OF HIGH AND LOW FREQUENCY LETTERS RESPECTIVELY
RESULT  R  IS A TABLE OF  N  GENERATRICES LISTED
ROWWISE IN DECREASING ORDER OF THE DIFFERENCE
BETWEEN THESE TWO COUNTS.
     ASSUMED AVAILABLE   ALPHABET   ABC
                         FUNCTION   SHIFT
```

```
⍝      * * * THWAITES' ADVERTISEMENT * * *

      ∇ MINMAX[⎕]∇
     ∇ R←N MINMAX TXT,MAX,MIN,AUX
[1]    MAX← ETAONIRSH
[2]    MIN← JKQXZ
[3]   SEARCH R←ABC SHIFT TXT
[4]    AUX←+/(R∊MAX)-(+/[⎕IO]R∊MIN
[5]    R←R[N↑⍒AUX;]
     ∇

      ⍝ SOLVING THE CRYPTOGRAM

      ⍝ ELIMINATING THE SIGNATURE 'VRBV' FOR THE TIME
      ⍝ BEING, WE THEREFORE HAVE THE KASISKI MATRIX

      ρ⎕←C7←7 KASISKI 4↓C
GZZESQV
TNSRXWV
FLOLXWV
QBOJZFX
HE BXQX
NOZEORB
XDUSDFR
TOYBMFX
YDUOBSL
JPTADRV
JPTGRST
WJZZ CE
JFLMOFF
ZLGUSCD
14 7

      ⍝ ASSUMING PLAINTEXT ALPHABETS WE APPLY THE
      ⍝ MINMAX LETTER FREQUENCY ANALYSIS

      ρ⎕←P7←KMETHOD C7
RYTHISR
OMMUNIR
ATIONIR
LAIMPRT
CEDENET
INTHEDY
SCOVERN
OFSECRT
TCORREH
PONDENR
EONTHEE
RINCIPA
EOFPERH
UTATION
14 7
```

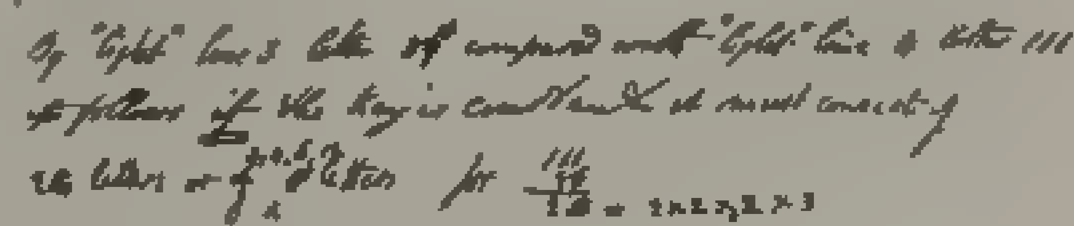


```
⍝      * * * THWAITES' SECOND LETTER * * *

      ⍝ LAST COLUMN INVESTIGATED
      ⎕←COL←4 MINMAX C7[;7]
RRRTTXNTHREABC
[redacted]
YYYAAEUADYLHIJ
CCCEEIYESCPLMN

      ⍝ INSERTING LAST ROW
      P7[;7]←COL[4;]
       P7
BYTHISCOMMUNICATIONICLAIMPRECEDENCEINTHEDISCOVERYOFSECRETCORRESP
      ONDENCEONTHEPRINCIPLEOFPERMUTATION

      ⍝ THWAITES DID APPLY FALSE WORD DIVISIONS

       ρ(RPT1 '6↑ρ' RESTORE ,P7), 4↑C
BYTHI, SC. OMMUNICATI. ONIC. LAINP.
RECEDEN. LEINTHE, DISCO, VE, RYOFSECR
ET. CORR. ESPO, NDEN, CEONTHEPR. INC,
IP, LEOFPERM, UTATION  -  VRBV

      ⍝ THE INTERPRETATION OF THE SIGNATURE IS EXPLAINED
      ⍝ IN THWAITES' LETTER.


⍝      * * * THWAITES' SECOND LETTER * * *

      ⍝ IN HIS SECOND LETTER TO THE JOURNAL OF THE SOCIETY OF
      ⍝ ARTS, NO. 95, VOL.2, SEPT. 15, 1854, THWAITES POSED HIS
      ⍝ CHALLENGE IN THE FORM OF THE CIPHER

      THWTS
UTHU, DGV, UKB LKZT LRWN.
FLHL HPG SVUS QR KFHWAZ I ORBNDW  EHA RJZZ THQJZ YIMEVURV
N VGWW HUCCJF NLSI, RBDJ PWE XLLGF ALAUDPX
TRVM XNR DGEHU KLLGF. SGR DMTU TPCM, N IEOGCM JGHJ
CTEW GOMW RAUPVH SB. HWKC TNVY GGVH HZSTG
FGZV XNFG XOTGNG FB M WSL, AM YZU JE
NVUJ AT. FPU KRWM AR W

      ⍝ WHICH, HE CLAIMED, ENCIPHERED THE FOLLOWING QUOTATION
      ⍝ FROM SHAKESPEARE'S 'THE TEMPEST' (ACT. 1, SCENE 2)

      TEMP
SOFT, SIR, ONE WORD MORE
THEY ARE BOTH IN EITHER'S POWERS. BUT THIS SWIFT BUSINESS
I MUST UNEASY MAKE, LEST TOO LIGHT WINNING
MAKE THE PRIZE LIGHT. ONE WORD MORE, I CHARGE THEE
THAT THOU ATTEND ME. THOU DOST HERE USURP
UPON THIS ISLAND AS A SPY, TO WIN IT
FROM ME, THE LORD ON T

      ⍝ THE PROBLEM HE SET C.[BABBAGE], WAS TO FIND THE KEY
```

```
⍝        ⍝ ⍝ ⍝ THWAITES' SECOND LETTER ⍝ ⍝ ⍝

⍝ DETERMINATION OF THE MASTERKEY

⍝ REMOVING PUNCTUATIONS, ETC , WE HAVE
⍴L←PUNCTUATION THWTS
9 399
⍴C←L REMOVE THWTS
213
⍴P←L REMOVE TEMP
213

⍝ SINCE BABBAGE ALWAYS WORKED IN 1-ORIGIN, LET US ASSUME
⎕IO←1

⍝ THEN HE FOUND THE  MASTERKEY  AS FOLLOWS
⍴K←ABC[(⍴ABC)|(ABC⍳C)-ABC⍳P]
213

⍝ OR, TO EMPHASIZE ITS PERIODICITY OF 24 LETTER,
⎕←K←24 KASISKI K
P QAK (EFWNOV HP CEI LEMGX
PQ JAKHDFWNJVHPYCEILDCMGX
BQQAKHEFWNOVHPYCEILDCMGX
HQCAKHDFWNOV HPYCE I  ECMGX
HWGAKHI  WNC VEP  EI I  M X
FQGAKHDFWNOVHPYCEILDEMGX
BQGAK I  WNL VHPYCE IL   MGX
HQGAKHDFWNOVHPYCEILDCMGX
HQGAKHDFWNGVHPYCEILDC

⍝ INSPECTION OF THE FIRST ROW IN THIS MATRIX, REVEALS THE
⍝ ERROR BABBAGE REFERRED TO, IN HIS SECOND LETTER TO THE
⍝ JOURNAL OF THE SOCIETY OF ARTS, NO. 98, VOL. 2, OCT. 6
⍝ 1854, WHEN HE REMARKED    THE SECOND LETTER  T  IN MR
⍝ THWAITES  CYPHER IS A MISTAKE,  IT SHOULD BE  F

⍝ CLEARLY, THIS  MASTERKEY
⍴⎕←K←K[2 ]
FQGAKHDFWNOVHPYCEILDCMGX

⍝ AGREES WITH BABBAGE S LISTING OF ITS ALPHABETIC INDICES
ABC⍳K
 17 7 1 11 8 4 6 23 14 15 22 8 16 25 3 5 9 12 4 3 13 7 24

⍝ EVIDENTLY,  BABBAGE DISCOVERED,  RUNNING IT DOWN THE
⍝ ALPHABET,  CONSULTING HIS DICTIONARIES,  ETC ,  THAT
⍝ IT WAS BASED ON SUPERPOSITION OF TWO OR MORE SUBKEYS

⍝ BABBAGE ON THE KEY PERIODICITY

⍝ EXAMINING THWAITES' CIPHER, BABBAGE AND HIS SON, HENRY
⍝ PREVOST, DISCOVERED THE BASIC PRINCIPLES OF WHAT NOW IS
⍝ KNOWN AS THE  KASISKI ANALYSIS , AND GAVE IT AN EXPLICIT
⍝ FORMULATION

⍝ THUS, ON A WORKSHEET DATED   18 SEP. 1854, BRIGHTON ,
⍝ BABBAGE WROTE (BL, ADD, MS  37205, FF. 138-139)    BY
⍝ 'LIGHT' LINE 3 LETTER 87 COMPARED WITH  LIGHT' LINE 4
⍝ LETTER 111 IT FOLLOWS IF THE KEY IS CONSTANT THAT IT
⍝ MUST CONSIST OF 24 LETTERS OR OF 3, 4, 6, 12 LETTERS
⍝ FOR  111 87 = 24 = 2×2×2×3
```



```
⍝        ⍝ ⍝ ⍝ THWAITES' SECOND LETTER ⍝ ⍝ ⍝

⍝ THIS NOTE IS FOLLOWED UP, FOR EXAMPLE, BY A DIGRAM TEST
⍝ FOR THE LETTER PAIR  'TH ,  REVEALING THE REPETITIONS,
⍝  HW  154-34 = 120 = 5×24    &    XH  175-103 = 72 = 3×24

⍝ ALSO, FOR ALL DISTANCES BETWEEN ANY TWO IDENTICAL CIPHER
⍝ LETTERS,  SATIFYING THAT BOTH ARE TRANSLATED BY THE SAME
⍝ PLAINTEXT LETTER.  BABBAGE CONFIRMS BY AN EXHAUSTIVE
⍝ SEARCH THAT THEY ARE ALL MULTIPLES OF 24

⍝ HENCE, WITH BABBAGE S PRIME FACTORIZATION
PRIMEFACTOR ⍴K

⍝ IT WOULD APPEAR THAT HE STIPULATED, FROM A GUESS OF ONLY
⍝ TWO SUBKEYS, THAT THEIR LENGTHS HAD TO BE EITHER
⍝        3 AND 8 ,      2 AND 12 ,     OR      4 AND 6

⍝ HARMONIC ANALYSIS

⍝ BABBAGE S WORKSHEETS CONTAIN A VARIETY OF EXPERIMENTS TO
⍝ ESTABLISH, WHAT IN MAXWELL S TERMINOLOGY MAY BE CALLED
⍝ THE CONDITIONS OF  'CONJUGATE KEYS .  FOR EXAMPLE, UNDER
⍝ THE HEADING    HENRY S CYPHER ,  WE FIND A COMPOSITE KEY
⍝ PRODUCED BY A FOUR TIMES REPETITION OF THE KEYWORD  TWO
⍝ AGAINST THE LETTER   P   (BL, ADD  MS  37205, F. 136).

⍝ PRESUMEABLY, BABBAGE DISCOVERED THAT THE LENGTH OF TH
⍝ COMPOSITE KEY OR  MASTERKEY  HAD TO BE THE   LCM   OR
⍝  LEAST COMMON MULTIPLE'  OF THE LENGTHS OF THE SUBKEYS

⍝ AS MAY BE FOUND IN ANY MATHEMATICS TEXTBOOK, THE LCM OF
⍝ TWO POSITIVE INTEGERS  'A' AND  B ,  IS AN INTEGER SUCH
⍝ THAT  (1)  LCM IS DIVISIBLE BY BOTH   A  AND  B ,  AND
⍝ (2) IF SOME OTHER INTEGER   X   IS ALSO DIVISIBLE BY
⍝ BOTH   A' AND  B ,  THEN   X   IS DIVISIBLE BY LCM TOO

⍝ A FUNCTION, GENERALIZING THIS NOTION TO A VECTOR OF
⍝ INTEGERS, MAY BE DEFINED

    CCLCM
THE LEAST COMMON MULTIPLE  L  OF A VECTOR  V  OF
INTEGERS, IS DETERMINED RECURSIVELY INVOKING, AT
EACH STEP, THE EUCLIDEAN ALGORITHM,
    ASSUMED AVAILABLE   FUNCTION  GCD

    ∇ LCM[⎕] ∇
  ∇ L←LCM V,⎕IO
[1]  ORIGIN ⎕IO←1
[2]   →END×1=⍴ V
[3]   V← (×/2↑V)÷GCD 2↑V),2↓V
[4]   L←1×LCM V
[5]   →0
[illegible]  END L←V
  ∇
```


By 'light' line 3 letter 87 compared with 'light' line 4 letter 111 it follows if the key is constant that it must consist of 24 letters or of 3, 4, 6, 12 letters for 111 − 87 = 24 = 2×2×2×3

(By permission of the British Library)

```
⍝ HERE, IN STATEMENT [3], WE HAVE INTRODUCED THE NOTION
⍝ OF  GCD , OR  THE GREATEST COMMON DIVISOR .  THE GCD
⍝ OF TWO POSITIVE INTEGERS   A  AND  B   IS AN INTEGER
⍝ THAT IS NOT ONLY A COMMON DIVISOR OF   A  AND  B ,  BUT
⍝ IT IS ALSO A MULTIPLE OF EVERY OTHER COMMON DIVISOR

⍝ A SPECIAL CASE OF PARTICULAR INTEREST, IS    GCD = 1 ,
⍝ BECAUSE THEN   A  AND  B   ARE  CONJUGATE ' OR, AS IT IS
⍝ EXPRESSED IN MATHEMATICS   RELATIVELY PRIME

⍝ AN ALGORITHM FOR DETERMINATION OF GCD OF TWO INTEGERS
⍝ WAS DEVELOPED BY THE PYTHAGOREANS IN ANCIENT GREECE
⍝ DESCRIBED BY EUCLID ABOUT 300 B C. IN HIS  ELEMENTS ,
⍝ IT IS KNOWN IN ALL TEXTBOOKS ON ALGEBRA AS   EUCLID S
⍝ ALGORITHM .  THUS

      ⍎GCD
THE EUCLIDEAN ALGORITHM IS EMPLOYED TO DETERMINE THE
GREATEST COMMON DIVISOR  D  OF VECTOR  V  OF INTEGERS

      ∇ GCD[⎕] ∇
    ∇ D←GCD V
[1]   V←|V
[ ]  N  F  0=, V
[3]   V←D,(0≠D|V)/D|V
[4]   → [≠ρV   NX]
    ∇

      ⍝ APPLYING THIS FUNCTION, WE FIND FOR THE THREE PAIRS
      ⍝ OF ALTERNATIVE SUBKEYS
      ( B 3 6

        1

      ⍝ 4 + 6

      ⍝ HENCE, ONLY THE PAIR    3 AND 8   IS RELATIVELY PRIME.

      ⍝ TO FIND THE LCM OF TWO INTEGERS   A  AND  B ,  THE
      ⍝ COMPUTATION MAY BE FORMULATED IN TERMS OF THE GCD
      ⍝               LCM ← (A×B) ÷ GCD A,B
      ⍝ THUS  TO ILLUSTRATE
       (8×3) ÷ GCD 3 8

      ⍝ THIS EXPLAINS STATEMENT [3] IN THE FUNCTION   LCM

      ⍝ THE INTERPRETATION OF THE LCM OF THE LENGTHS OF TWO
      ⍝ SUBKEYS, IS THE LENGTH OF THEIR COMPOSITE KEY, SAY
      LCM 3 8

      LCM 4 6

      ⍝ CONSEQUENTLY, ONLY THE TWO SUBKEYS OF LENGTHS   3 AND 8
      ⍝ WILL PRODUCE A  MASTERKEY' OF LENGTH 24.  NOTE, THOUGH,
      ⍝ THAT THIS PRESUPPOSES THAT THEY ARE NOT SOME MULTIPLES
      ⍝ OF THE TWO NUMBERS
      LCM 6 8
```



```
      ⍝ COMPARISONS OF PERIODICITY

      ⍝ FOLLOWING BABBAGE, WE NOW COMPARE THE PERIODICITY OF THE
      ⍝  MASTERKEY   WITH THOSE OF TWO SUBKEYS OF THE ASSUMED
      ⍝ LENGTHS   3 AND 8'  RESPECTIVELY
      PRINT M←3 24⍴(⍳24),(24⍴⍳3),24⍴⍳8
 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
 2 3 1 2 3 1 2 3 1  2  3  1  2  3  1  2  3  1  2  3  1  2  3
 2 3 4 5 6 7 8 1 2  3  4  5  6  7  8  1  2  3  4  5  6  7  8

      ⍝ THE IMPORTANT OBSERVATION TO BE MADE HERE, IS THAT IF
      ⍝ WE PICK THOSE COLUMNS FOR WHICH ONE OF THE SUBKEYS HAS
      ⍝ THE SAME LETTER (NUMBER 1, SAY), THEN THE  MASTERKEY
      ⍝ WILL DETERMINE THE LETTERS OF THE OTHER SUBKEY, APART
      ⍝ FROM A CHANGE OF LEVEL (CYCLIC SHIFT OF THE ALPHABET).

      ⍝ KEYWORD OF LENGTH 3

      ⍝ CONSIDERING THOSE COLUMNS FOR WHICH THE SUBKEY OF LENGTH
      ⍝ 8 HAS THE SAME NUMBER 1, WE FIND
      ⎕←M3←M[ (1=M[3 ]) /⍳ 1↑⍴M]
  1  9 17
  1  3  2
  1  1  1
      ⍝ SO CONSEQUENTLY A GENERATRIX OF THE KEY IS
      ⎕←K3←K[⎕←M3[1,⍋M3[2,]]]
1 17 9
NEW

      ⍝ RUN DOWN THE ALPHABET, THIS KEY HAS THE INTERPRETATIONS
      ⍝  LOG  AND  RUN , MENTIONED BY BABBAGE, IN ADDITION TO
      ⍝ THE WORD  TWO  APPLIED BY THWAITES   THUS,
      ABC SHIFT K3
NEW
OFX
PGY
QHZ
RIA
SJB
TKC
ULD
VME
WNF
XOG
YPH
ZQI
ARJ
BSK
CTL
DUM
EVN
FWO
GXP
HYQ
IZR
JAS
KBT
LCU
MDV
```

```
⍝          * * * THWAITES  SECOND LETTER * * *

      ⍝ KEYWORD OF LENGTH 8

      ⍝ REPEATING THE PROCEDURE FOR THE OTHER SUBKEY, WE FIND
      ⎕←M8←M[ ,1=M[2 ]  , 1↑⍴M]
  1   4   7 10 13 16 19 22
  1   1   1  1  1  1  1  1
  1   4   7  2  5  8  3  6
      ⎕←K8←K[⎕←M8[1 ⍋M8[3,]]]
1 10 19 4 13 22 7 16
BNLAMMDC
      ⍝ SIMILARLY, RUNNING THIS KEY DOWN THE ALPHABET, WE SEE,
      ⍝ AS DETERMINED BY BABBAGE, THAT THE OTHER KEYWORD IS
      ⍝  COMBINED , THUS.
      ABC SHIFT K8
BNLAMMDC
COMBINED
DPNCJOFE
EQODKPGF
FRPELQHG
GSQFMRIH
HTRGNSJI
IUSHOTKJ
JVTIPULK
KWUJQVML
LXVKRWNM
MYWLSXON
NZXMTYPO
OAYNUZQP
PBZOVARQ
QCAPWBSR
RDBQXCTS
SECRYDUT
TFDSZEVU
UGETAFWV
VHFUBGXW
WIGVCHYX
XJHWDIZY
YKIXEJAZ
ZLJYFKBA
AMKZGLCB
```



```
      ⍝          * * * BABBAGE S CHALLENGE * * *

      ⍝ IN HIS SECOND LETTER TO THE JOURNAL OF THE SOCIETY OF
      ⍝ ARTS, NO. 98, VOL. 2, OCT. 6, 1854, BABBAGE SET THWAITES
      ⍝ THE COUNTER CHALLENGE OF FINDING THE KEY TO THE CIPHER

      BBG
JEXC, WII, HDX IVOW LQUQ,
NNKA WES VMGE FX WADGZJ'H OXQHOW  LGP SVRG VWMFI HRZ8DMJJ
A SFWP RECLCZ ZNFE. CQKX DWM MEKRG XFXXALD
XKRH MXH ITPVW UGTZY, YBC RUIG CGZT, F SDXTCV WLXM
KKNG XQLQ SDLISP CI. GEXS TSAQ IWMH PEDOM
ZRAA FOCV GQXDRS XU Q CA8, RY LSX HW
FKQP ZZ, GNH LYRH WJ'K.

      ⍝ ENCIPHERED FROM THE SAME PASSAGE OF SHAKESPEARE.

      ⍝ SINCE WE HAVE ALREADY THE PLAINTEXT 'P' AVAILABLE IN A
      ⍝ CLEANED FORM, WE PROCEED DIRECTLY TO THE CRYPTOGRAM
      ⍴C←L REMOVE BBG
213

      ⍝ FURTHER, FOR CONVENIENCE WE ASSUME THROUGHOUT A 0 ORIGIN
      ⎕IO←0

      ⍝ A PERMUTED CIPHER ALPHABET?

      ⍝ IF BABBAGE HAS USED A STANDARD ALPHABET, HIS  MASTERKEY
      ⍝ SHOULD BE
      ⎕←K←ABC[(⍴ABC)|(ABC⍳C)-ABC⍳P]
ROSJEARTQTMHXTZCDNJGBCWNDUYNXKKSSKZVSPZJUDXETHWZDJUIAEAPGXHIGIRR
      SGLEWXRYLKBNNVARMSEKIYBWEKNBXKKBYXLKMDTQLTCHWSJYNSFKOYVGRD
      QSIPXQWXCWRDETIRDNNEJDWSKSEFMQENXJYQEIXBSVDVMJXYFCMNNHLDYY
      MDEFKLDKLDIKTKKZDATCDNVNLIAKAEIWR

      ⍝ NEGLECTING THE POSSIBILITY OF A KEYLENGTH EQUAL TO THE
      ⍝ TOTAL LENGTH OF THE PLAINTEXT, WE CONCLUDE THAT HE HAS
      ⍝ USED A PERMUTED CIPHER ALPHABET  XYZ .

      ⍝ KASISKI ANALYSIS

      ⍝ SINCE THE PERIODICITY OF THE KEY IS ONLY REVEALED BY THE
      ⍝ REPEATED DIGRAMS, IT IS FORTUNATE THAT COMPARISON WITH
      ⍝ THE PLAINTEXT PROVIDES A SHORT CUT TO A SPEEDY SOLUTION

      ⍝ THUS, WE FIND A PERIODICITY OF 63 FOR THE COMPOSITE KEY
      ⎕←C63←63 KASISKI C
JEXCWIIHDXIVOWLQUQNNKAWESVMGEFXWADGZJHOXQHOWLGPSVRGVWMFIHRZQIM
JASFWPRECLCZZNFECQKXDWMMEKRGXFXXALDXKRHMXHITPVWUGTZYYBCRJIGCGZT
FSDXTCVWLXMKKNGXQLQSDLISPCIGEXSTSAQIWMHPEDOMZRAAFOCVGQXDRSXUQCA
BRYLSXHWFKQPZZGNHLYRHWJK

      ⍝ WHICH COMPARES WITH THE PLAINTEXT MATRIX
      ⎕←P63←63 KASISKI P
SOFTSIRONEWORDMORETHEYAREBOTHINEITHERSPOWERSBUTTHISSWIFTBUSINES
SIMUSTUNEASYMAKELESTTOOLIGHTWINNINGMAKETHEPRIZELIGHTONEWORDMORE
ICHARGETHEETHATTHOUATTENDMETHOUDOSTHEREUSURPUPONTHISISLANDASASP
YTOWINITFROMMETHELORDONT
```

```
      ⍝ FOR INSTANCE, OBSERVE THE REPEATED LETTER COMBINATIONS
      ⍝ IN COLUMNS SUCH AS,
      [,3 27+⍳4]
GFFX
FXF
⍳L+S

      [;8+ /+ ⍳]
THIN
TWIN
THOU


      ⍝ SYMMETRY OF POSITION

      ⍝ THE FACT THAT ALL LETTERS IN A COLUMN OF THE KASISKI
      ⍝ MATRIX ARE TRANSLATED BY THE SAME ALPHABET, IS THE
      ⍝ ENTRANCE NEEDED TO DETERMINE THE CIPHER ALPHABET  XYZ

      ⍝ THE TECHNIQUE TO BE APPLIED FOR THIS PURPOSE, WAS
      ⍝ INTRODUCED BY AUGUSTE KERCKHOFF IN HIS BOOK   LA
      ⍝ CRYPTOGRAPHIE MILITAIRE , PUBLISHED 1883   KNOWN AS
      ⍝ THE  SYMMETRY OF POSITION , IT MAY BE IMPLEMENTED

      CCSYMPOS
THE CIPHER ALPHABET 'R  IS DETERMINED BY THE SOCALLED
 SYMMETRY OF POSITION  COMPARING THE KASISKI MATRIX OF
THE CRYPTOGRAM (I.E., LEFT ARGUMENT  KC ) WITH THAT OF
THE PLAINTEXT (I E., RIGHT ARGUMENT  KP ), RESULT  R
MAY BE A TABLE OF NON-RELATED SUBALPHABETS LISTED IN
ARBITRARY ROW ORDER. UNKNOWN LETTERS IN THE PLAINTEXT
ARGUMENT  KP  MAY BE PADDED WITH BLANKS DISREGARDING
ANY CORRESPONDING CHANGE OF THE ARGUMENT  KC
          GLOBAL VARIABLE    ALPHABET  ABC

      ∇ SYMPOS[⎕] ∇
    ∇ R←KC SYMPOS KP;⎕IO;AUX;N;I;SUB
[1]  ORIGIN ⎕IO←1
[2]   →(∧/ ⍴KC =⍴KP)/ 0
[3]  TABLEAU R←((¯1↑⍴KC)×⍴ABC)⍴0
[4]   I←' '≠,⍉KP
[5]   AUX←I  ⍉ ABC KP ←(⍴KC ⍴⍴ABC)× 1+  ⍳↑⍴KC
[6]   R[AUX]←I/,⍉(1+⍴ABC)|ABC⍳KC
[7]   R←((¯1↑⍴KC),⍴ABC)⍴R
[8]  COMPARE N←0
[9]   AUX←((⍳⍴ABC)∊R)/⍳⍴ABC
[10] NXT N←N+1
[11]  →(N>⍴AUX)/END
[12]  I←+/∨\⍉R=AUX[N]
[13]  S UB←  0≠I  [ ] ⍉∨0≠I⌿R
[14]  R← (0=I /R) ⍪ [1]+/ ⍪[I← \0≠SUB
[15]  →(  1↑⍴R) END
[16]  →NXT
[17] END R←(' ',ABC)[1+R]
    ∇
```



```
      ⍝ TO ILLUSTRATE THE METHOD, LET US CONSIDER, SAY
      ⎕←CT←C63[ 12+⍳14]
OWLGUQNNKAWESV
ZNFEFGKXDWMMEK
KNGXGUQSDLISPC
ZZGNHLYRHWJK
      ⍝ WHOSE CORRESPONDINGLY GUESSED (HERE, KNOWN) PLAINTEXT
      ⎕←PT←P63[ 12+ 14]
RPMORETHEYAREB
MAKE E TTO R I
HATTHO ATTENDM
METHELORDONT
      ⍝ WE PAD WITH BLANKS TO DEMONSTRATE THAT WE NEED NOT
      ⍝ HAVE GUESSED ALL LETTERS
      PT[I,8 9]←' '
      PT
RPMORETHEYAREB
MAKELEST  OLIG
HATTHOUATTENDM
METHELORDONT

      ⍝ NOW, INTRODUCING THE STOP CONTROL
      S∆SYMPOS←8 15
      ⍝ WE INVOKE THE FUNCTION
      XYZ←CT SYMPOS PT

SYMPOS[8]
      ⍝ AT THIS STAGE WE HAVE A TABLE SHOWING ROWWISE, IN ORDER
      ⍝ OF THE COLUMNS OF THE KASISKI MATRIX, THE CORRESPONDING
      ⍝ CIPHER ALPHABETS
      ⍴⎕←(    ABC)[1+R]
  K     Z     D
N  WZ
        F L      G
   E  N     Q    X
   H  Q   C     L
   Q      L  U
             Y   KNQ
S     N         R X
  HK              D
             W    L     A
W   I       JM
          M S   E K
  PS   E
 V    K      C
14 26
      →⎕LC

SYMPOS[15]
      ⍝ TOGETHER THESE ALPHABETS COMPRISE THE FOLLOWING LETTERS
      ⍴⎕←ABC[AUX]
ACDEFGHJKLMNOPQRSUVWXYZ
23
```

```
      ⍝ WE NOW PROCEED BY AN ITERATIVE PROCEDURE, TAKING ONE OF
      ⍝ THESE LETTERS AT A TIME, IN ORDER TO DETERMINE AND TO
      ⍝ COMBINE TO A SINGLE ALPHABET THE SUBSET OF ALPHABETS
      ⍝ HAVING THE LETTER UNDER CONSIDERATION IN COMMON

      ⍝ THUS  CONSIDERING THE FIRST LETTER
      ABC[AUX[N]]
A

      ⍝ IT IS FOUND IN THE ALPHABETS
      ⍴⎕←      ABC [I+S]B
A                 W     L
I 26

      ⍝ CLEARLY  THIS WILL NOT CHANGE THE TABLE, SO WE PROCEED
      ⍝ WITH THE SECOND LETTER
      →⎕LC

   N              J
      ⍝ THE NEW LETTER IS
      ⍝

      ⍝ WHICH IS FOUND IN THE ALPHABETS
      ⍴⎕←      ABC [     ]
                       H   G
C                   V      H

      ⍝ IT FOLLOWS THAT THE TABLE MAY BE REDUCED, COMBINING THE
      ⍝ TWO ALPHABETS CONTAINING LETTER  C   AND PLACING THE
      ⍝ RESULTING ALPHABET AS THE LAST ROW
      ⍴⎕       ABC [I;R]
       K      Z      O
N   WZ
             F L         G
     E   N         Q      X
     Q        L   U
                   Y     KNQ
S        N            R  X
   HK                    D
W    I           JM
            H S T  E  K
   PS
A                 W     L
C      U           V    HK  Q
13 26
      ⍝ THIS EXPLAINS THE PRINCIPLE UNDERLYING THE FUNCTION, SO
      ⍝ WE REMOVE THE STOP CONTROL
      SΔSYMPOS←⍳0
      ⍝ AND CONTINUE THE EXECUTION OF THE FUNCTION
      →⎕LC

      ⍝ THE RESULTING ALPHABET IS
      ⍴⎕←X
Q WZCFILORJXADGJMPSVY EHKN
I 26
      ⍝ WHICH REVEALS TWO UNIDENTIFIED LETTERS
```



```
      ⍝ ROTATED TO BEGIN WITH LETTER  A
      ⎕←XYZ←,((,XYZ)⍳'A')⌽XYZ
ADGJMPSVY EHKNQ WZCFILORUX
      ⍝ IT IS IMMEDIATELY EVIDENT THAT IT WAS PRODUCED
      ⍉9 3⍴ABC
ADGJMPSVY
[illegible]
CFILORJX

      ⍝ HENCE, BABBAGE S CIPHER ALPHABET IS '
      ⍴⎕←XYZ← 14 ⍉9 3⍴ABC
ADGJMPSVYBEHKNQTWZCFILORJX
26

      ⍝ BABBAGE S COMPOSITE KEY

      ⍝ WE ARE NOW ABLE TO DETERMINE BABBAGE S  MASTERKEY :
      ⍴⎕←K←63 KASISKI ABC[(⍴ABC)|(XYZ⍳C)-ABC⍳P]
LEUZYMDXOVYTFNJAHKJGICQTCGQJDLMMSIVNMTHLSHFYXIMNAPKPLWODKDZGOAL
LSUZYMIXOVATFNJGHKLGICQTCQQJDLMMSIVNMNHLSHFYXIMNJJKPUWJBKTZGJAL
LEUZYMDXOVATFNJGHKJGICQTCGQJDLMMSIVNMNHLSHFYXIMNAPKPLWLBKDZGOAL
LEUZYMIKOVATFNJGHKLGICQT
4 63
      ⍝ TO AVOID ENCIPHERMENT ERRORS, WE TAKE THE THIRD LINE
      ⍴⎕←K←K[3;]
LEUZYMDXOVATFNJGHKJGICQTCGQJDLMMSIVNMNHLSHFYXIMNAPKPLWOBKDZGOAL
63

      ⍝ A PRIME FACTORIZATION OF THE KEY LENGTH YIELDS
      PRIMEFACTOR ⍴K
 3 7
 2 1
      ⍝ HENCE, THERE ARE TWO POSSIBILITIES, NAMELY    7 AND 9
      ⍝ AND    3 AND 21 ,   THE LCM S OF WHICH ARE
      LCM 7 9
63
      LCM 3 21
21
      ⍝ WHICH ELIMINATES THE LAST POSSIBILITY

      ⍝ THE PERIODICITY OF TWO KEYWORDS OF LENGTHS 7 AND 9, ARE
      ⍴M←3 63⍴(⍳63   63⍴ 7) 63⍴⍳9
3 63

      ⍝ KEYWORD OF LENGTH 7

      ⍝ PROCEEDING AS WE DID FOR THWAITES' CIPHER,
      ⍴⎕←M7←M[  ; M[2 ] ⍳ 1↑⍴M]
  1 10 19 28 37 46 55
  1  3  5  0  2  4  6
  1  1  1  1  1  1  1
3 7
      ⍴⎕←K7←(K[2,])[⎕←M7[0,⍋M7[1,]]]
28 1 37 10 46 19 55
NENAMOB
7
```

```
⍝          * * * BABBAGE'S CHALLENGE * * *

      ⍝ NEGLECTING TO RECORD A LITTLE EXPERIMENTATION WE FIND
      ⍝ THAT IT IS IDENTIFIED BY RUNNING DOWN THE ALPHABET  ABC
      ⍴⎕←ABC SHIFT ABC[XYZ⍳K7]
BKNAECJ
C[illegible]CHFDK
DMPCGEL
ENQIHFM
FOREIGN
[illegible]
HQTGKIP
[illegible]
JSVIMKR
KTWJNLS
LUXKOMT
[illegible]
NWZMQOV
[illegible]
PYBOSQX
QZCPTRY
RADQUSZ
S[illegible]VTA
TCFSWUB
[illegible]
VEHUYWD
WFIVZXE
XGJWAYF
YHKXBZG
ZILYCAH
AJMZDBI
26 7

      ⍝ THUS, THE KEYWORD OF 7 LETTERS IS
      ⍴⎕←K7←(4⌽ABC)[XYZ⍳K7]
FOREIGN
7

      ⍝ KEYWORD OF LENGTH 9

      ⍝ SIMILARLY, WE HERE PROCEED AS FOLLOWS
      ⍴⎕←M9←M[,(1=M[1;])/⍳¯1↑⍴M]
  1  8 15 22 29 36 43 50 57
  1  1  1  1  1  1  1  1  1
  1  8  6  4  2  0  7  5  3
3 9
      ⍴⎕←K9←(K[2;])[⎕←M9[0,⍋M9[2;]]]
36 1 29 57 22 50 15 43 8
MELDQKOYG
9
```



```
⍝          * * * BABBAGE'S CHALLENGE * * *

      ⍝ AFTER SOME EXPERIMENTATION WE FIND THAT IT SHOULD BE
      ⍝ DETERMINED RUNNING DOWN THE ALPHABET  XYZ' OF THE
      ⍝  DUAL  EXPRESSION OF THAT OF THE 7 LETTER KEYWORD
      ⍴⎕←XYZ SHIFT XYZ[ABC⍳K9]
KMHJWESJG
NPKNZHVXT
GSNPCKYAW
TVQSFNBDZ
W[illegible]TVIQEGC
ZBWYLTHJF
CE[illegible]BOWKMI
FHCERZNPL
IKFHUCQSO
LNIKXFTVR
OQLNAIWYU
RTOQDLZBX
UWRTGOCEA
XZUWJRFHD
ACXZMUIKG
DFACPXLNJ
GIDFSALQM
JLGIVDRTP
ML[illegible]LYGUWS
PRMOBJXZV
SUPREMACY
VXSUHPDFB
YAVXKSGIE
BDYANVJLH
EGBDQYMOK
HJEGTBPRN
26 9

      ⍝ THUS, THE KEYWORD OF 9 LETTERS IS
      ⍴⎕←K9←(20⌽XYZ)[ABC⍳K9]
SUPREMACY
9
```

Epilogue

Man's life, we are told, is ruled by four passions. Two of them, being either fattening or immoral, can immediately be dispensed with. Of the remaining two, so the history of science bears out, creativity comes second. For it is spurred on by a craving for understanding

By instinct or conscious intent, the goal becomes perspective and wisdom To some, this is found in their chosen field, emanating from the particular studies of their training and profession. Others, perhaps by nature more rebellious, refuse lifelong confinement to the field they were reared in. Yet, by widening the scope, they are subject to adverse criticism from the professionals encamped on their few or many frontiers. This is a calculated risk, a foreseeable charge, which they find honourable to face.

The life and work of Charles Babbage, set forth in this tale, place him among the latter. Ostensibly about a cipher and APL, the story was actually about his secret. Lying dormant in his cryptogram for more than a century and a quarter, the secret was, as he himself so triumphantly announced it, *"foreign supremacy"*.

To interpret this statement, it must be recalled that, at heart, the great Victorian scientist and pioneer was a university man. Long ago, the university was born of the Catholic Church Today, the view may no more be *"sub specie æternitatis"*, in the perspective of eternity, but hopefully the aim has not changed. Throughout life, Babbage never lost it. This is why his ideas on computing combined with modern technology, so drastically is changing our society. The core of these ideas are in the mainstream of scientific development. To explain them, in particular on two accounts, was a central theme of our tale.

On one hand, there is the geometrical conception of data. Measurement and data are basic to all sciences and their applications. Across the disciplines, we find the same ideas of geometrical arrays, of symmetry and invariance, and of the fundamental scale-forms. Applied to data, Klein's century-old Erlanger Program captures what intuitively we might perceive, or perhaps even know. By invoking this program, our knowledge of data is organized and extended for use, and a

geometrical theory of data is created that is teachable and testable. It bespeaks Babbage's greatness as a scientist that he took this path and had the foresight to exploit it.

On the other hand, there is the experimental approach, using the computer as a tool of exploration – a computational laboratory. It is experiment, fertilized by intuitive and imaginative thoughts, that generate models and theories. But it is also by experiment, so-called prototyping, that we design new systems and enter into novel applications. As a workbench, the computer is a double-edged tool. We may employ it to improve our insight. But we may also use it to enhance our creative abilities. Babbage's writings document that he was well aware of these dual possibilities. This demonstrates his remarkable intuition and inventiveness.

The interactive APL terminal provides a workbench for dealing with the geometrical conception of data. Cryptography supplies an intriguing area of application. Together, they form a fascinating platform for the training of mind and skills. On the "testimony" of the celebrated mathematicians who appeared in this tale, we have here a playground for the winning of future battles.

On the wall of the playing field at Rugby School, there is a famous tablet. It commemorates an event which took place almost simultaneously with the publication of Babbage's plans for his Difference Engine. The tablet says

This stone
commemorates the exploit of
William Webb Ellis
who with a fine disregard for the rules of football
as played in his time
first took the ball in his hands and ran with it
thus originating the distinctive feature of
the Rugby Game
A.D. 1823

Babbage also invented a game – and with fine disregard for the rules set by his time. This game, he left for us to enjoy. To play it, is to share his secret.

NOTES, REFERENCES, AND ACKNOWLEDGEMENTS

The Philosophy of Decyphering

1) In a letter of August 3, 1985, Alfred W. Van Sinderen has kindly informed me that, apart from the collection of Babbage papers in the British Library, there exists quite a lot of Babbage's correspondence on ciphers at various places, and that he himself has some of these letters in his Babbage collection. Further, according to Van Sindern, Babbage made comments on a proposed "*paper on cyphers*" on more than one occasion in these letters. The problem of geographical distance prevented me from a closer study of this material. The reader interested in general in the printed papers of Charles Babbage may be referred to Van Sinderen's annotated bibliography (*Annals of the History of Computing*, Vol. 2, No. 2, April 1980, pp. 169-185). In this connection I would also like to mention the astonishing new finds, reported by Garry J. Tee, of Babbage relics: manuscripts, engine parts, etc., inherited by descendants of Babbage in New Zealand and Australia (*Annals of the History of Computing*, Vol. 5, No. 1, January 1983, pp. 45-59).

2) Charles Babbage: "Scientific Papers: 1. On cyphers and decyphering, 14. April 1808 – 12. February 1870". *British Library*, Additional Manuscripts 37205, Folios 1-305.

3) Charles Babbage: *Passages from the Life of a Philosopher*, London, 1864. Reprinted by Augustus M. Kelley, New York, 1969. See also P. Morrison & E. Morrison: *Charles Babbage and His Calculating Engines – Selected Writings by Charles Babbage and Others*. Dover Publications, Inc., New York, 1961.

4) The long-standing puzzle of Babbage's year and place of birth was solved only after a diligent search in parish registers. See Antony Hyman: *Charles Babbage – Pioneer of the Computer*, Oxford University Press, Oxford 1982.

5) A simulation in APL of Babbage's description and use of the Difference Engine is given in my article: "Mr. Babbage, the Difference Engine, and the Problem of Notation – An Account of the Origin of Recursiveness and Conditionals in Computer Programming". *Int. J. Engn. Sci.*, Vol. 19, No. 12, 1981, pp. 1657-1694.

6) See notes 1 and 3.

7) BL, Add Ms.37205, FF. 134-136.

8) I am indebted to the Royal Society of Arts for permission to bring this reprint. Simultaneously, I wish to express my gratitude to Dr. D.G.C. Allan, Curator-Librarian of the Society, for his invaluable assistance in trying to disentangle the relations between Babbage and the Society. The reprint does not include a brief letter which Thwaites communicated to the Journal of the Society of Arts, telling that he intended to answer the (first) letter by C. (Babbage) in the next issue.

9) Francis Baily: *An Account of the Rev'd John Flamsteed, The First Astronomer-Royal.* Lords Commissioners of the Admiralty, London, 1835, Appendix, pp. 348-349 & Introduction to the British Catalogue, pp. 390-391.

10) Dionysius Lardner: "Babbage's Calculating Engine." *Edinburgh Review,* No. CXX, July, 1834. Reprinted in P. Morrison & E. Morrison: *Charles Babbage and His Calculating Engines,* Dover Publications, Inc., New York, 1961, pp. 163-224. It may be of interest to know that this article was the only inspiration and source, guiding Georg and Edvard Scheutz in their design of the Swedish Difference Engine.

11) Charles Babbage: *The Exposition of 1851 or, Views of the Industry, the Science, and the Government of England.* Sec Ed., with Additions. John Murray, London, 1851, pp. 259-261.

12) BL, Add Ms. 37205, FF 81-130.

13) BL, Add Ms. 37205, FF 116.

14) BL, Add Ms. 37205, FF 123-124.

15) BL, Add Ms. 37205, F 125.

16) BL, Add. Ms. 37205, F 106.

17) BL, Add Ms. 37205, FF 86-88.

18) I am grateful to Mrs. E. Norsbo, sworn translator and interpreter, for indispensable help clarifying this and many other points, relating to the Victorian society of Great Britain.

19) I. B. Lindenfels: *Den hemmelige Skrivekonst eller, Chiffrer- og Dechiffrer-Konsten.* Fr. Brummers Forlag, Kjøbenhavn 1819.

20) C. A. Schou & T. Vogel-Jørgensen (eds.): *Illustreret Dansk Konversations Leksikon,* Bd. 18, Berlingske Forlag, København 1936, pp. 331-332. Jan Steenberg: *Rundetårn,* Nationalmuseet, Rhodos, København 1962.

21) J. V. Teisen & Louis Bobé (eds.): *Danmarks Adels Aarbog,* 54. årg., A/S J. H. Schultz Forlagsboghandel, København, 1937, pp. 43-47, 51-53 & [illegible].

22) Jens Johansen: *Frederik VI's Hær 1784-1814.* Udgivet af Generalstaben. I kommission hos N. Olaf Møller, København 1948.

23) BL, Add Ms. 37205, FF 210-213.

24) BL, Add Ms. 37205, F 240.

25) David Kahn: *The Codebreakers – The Story of Secret Writing,* Weidenfeld & Nicholson, London 1967, gives this year as 1850. However, as I interpret Babbage's handwriting, it is 1858 – a year which is also in better agreement with the dates of the associated correspondence with Mrs. Green.

26) The Harleian Collection refers to the manuscripts and legal documents formed by Robert Harley, 1st Earl of Oxford, and his son Edward Harley, 2nd Earl of Oxford. Purchased by the British Government in 1753 the collection is now in the Manuscripts Department of the British Library. The State Paper Office papers are housed in the Public Record Office, Kew, Richmond, Surrey.

27) Ronald Williams: *Montrose, Cavalier in Mourning.* Barrie & Jenkins, London, 1975. Winston S. Churchill: *A History of the English-Speaking People,* Vols. I-IV, Cassell & Co., Ltd., London, 1957.

28) BL, Add Ms. 37205, F 216.

29) W. T. Jeans: *Lives of the Electricians,* Whittaker & Co., London, 1887, pp. 219-221. David Kahn (*op.cit.,* note 25) claims by a reference to BL, Add Ms. 37205, folio 211, that in fact Babbage recommended Wheatstone. Folio 211, however, is the draft of the letter to Mrs. Everett Green, transcribed in figure 8B. As far as I have been able to ascertain from a microfilm from the British Library (supposed to contain the entire file of Add. Ms. 37205) none of Babbage's papers on deciphering supports this assertion.
I am indebted to Dr. J. Efstathiou, Queen Mary College, University of London, who, going through the original file in the British Library, confirmed my observation.

30) Brian Bowers: *Sir Charles Wheatstone.* Science Museum, Her Majesty's Stationary Office, London 1975, pages 185 & 233.

31) The anonymous article, which Kahn suggests might have been written by Babbage, was entitled: "Ciphers and Cipher-Writing", *MacMillan's Magazine,* Vol. XXIII, 1871, pp. 328-338.

32) M. R. Williams: "The Scientific Library of Charles Babbage", *Annals of the History of Computing,* Vol. 3, No. 3, July 1981, pp. 235-240.

33) I am indebted not only to Professor M. R. Williams for additional information on Babbage's private library, but also to the Librarian of the Crawford Library for supplying me with a photostatic copy of the entire catalogue prepared by R. Tucker for the sale of the "*Mathematical and Scientific Library of the late Charles Babbage,*" C. F. Hodgson & Son, London, 1872.

34) Reprinted by Frank Cass & Co., Ltd., London, 1970.

35) O. F. Morshead (ed).: *The Diary of Samuel Pepys – Selections.* Harper Torchbooks, New York, 1960, pp. 239-240.

36) Louis Trenchard More: *Isaac Newton – A Biography,* Dover Publications, Inc., New York, 1962, pp. 496-499.

37) Kai Christensen: "Sir Christopher Wren – videnskabsmand og arkitekt", Berlingske Tidendes Kronik, 26. October 1983.

38) Clark Emery: "John Wilkins' Universal Language". *ISIS*, Vol. 38, 1947-48, pp. 174-185.

39) I am indebted to Dr. Janet Efstathiou, Queen Mary College, University of London, for her assistance searching old issues of *The Times* in the university library.

40) BL, Add.Ms. 37205, FF 131-132

41) BL, Add.Ms. 37205, FF 17, 20-31. Apparently Babbage did not subscribe to these two newspapers, but copied the enciphered advertisements from some bound volumes, to which he referred explicitly by remarks such as: "*Original in Firebrand, Vol. VII, page 655*" (folio 27), simultaneously as he marked nearly all the translations at the bottom "*Copied*". An alternative interpretation of his notes may be that he obtained the translations from Firebrand. Thus his original list of references (folio 17) carries the designations "*F.B.*" and "*Trans.*", but it is not clear whether the latter term should mean "transcript" or "translation". The former interpretation, which I assume to be true, is supported by a worksheet (folio 22) with a letter frequency count and other computations, indicating attempts to break the cipher. Against it the latter interpretation is strengthened by the existence of a later list (folio 27), supplementing the references of the original by identification of the newspapers.

42) The enciphered advertisements illustrating the APL terminal session of this chapter, are all reproduced by permission of the British Library.

43) O. I. Franksen. "Are Data-Structures Geometrical Objects?" *Syst.Anal.Model.Simul.*, Vol. 1, 1984. Part I: "Invoking the Erlanger Program", No. 2, pp. 113-130; Part II: "Invariant Forms in APL and Beyond", No. 2, pp. 131-150; Part III: "Appendix A: Linear Differential Operators", No. 3, pp.249-258; Part IV: "Appendix B: Logic Invariants by Finite Truth-Tables", No. 4, pp. 339-350.

44) A.J. Perlis & S. Rugaber: "Programming with idioms in APL". *APL Quote Quad*, Vol. 9, No. 4, 1979, pp. 232-235.
T. P. Holls (ed.): "APL Programming Guide: Vector Operations". First Ed. International Business Machines Corp., Publ. No. G320-6103-0, New York, 1978.
T. Kunnas (ed.): "FinnAPL Idiom Library". Finnish APL Association, Helsinki, Oct. 8, 1981.

45) K. E. Iverson: "Elementary Algebra". IBM Philadelphia Scientific Center, Technical Report No. 320-3001, June 1971.

Between Mathematics and Reality

1) Charles Babbage: "Essays on the Philosophy of Analysis". Autograph. BL, Add.Ms. 37202, FF. 1-172. The statement on their presentation to the Cambridge Philosophical Society is given on folio 5.

2) J. M. Dubbey: *The Mathematical Works of Charles Babbage*. Cambridge University Press, Cambridge, 1978. See also I. Grattan-Guinness. "Essay Review of J. M. Dubbey's The Mathematical Works of Charles Babbage". *The British Journal for the History of Science*, Vol. 12, No. 40, 1979, pp. 82-88.

3) G. Polya: *How to Solve It*. Sec. Ed., Doubleday Anchor Books, Doubleday & Co., Inc., N.Y., 1957.

4) Charles Babbage: "Notation". *The Edinburgh Encyclopedia*, Vol. 15, 1830, pp. 394-399.

5) Charles Babbage: "On the Influence of Signs in Mathematical Reasoning". *Cambridge Phil. Soc. Trans.*, Vol. II, 1826, pp. 325-377.

6) Charles Babbage: "Observations on the Notation employed in the Calculus of Functions". *Cambridge Phil Soc. Trans*, Vol. I, 1820, pp. 63-76.

7) According to Cajori, Stifel in 1553 even "understood that a quantity with the exponent zero had the value 1". See Florian Cajori: *A History of Mathematical Notations*. Vol. I: *Notations in Elementary Mathematics*. The Open Court Publishing Co., La Salle, Illinois, 1928. Paperback edition 1974.

8) Morris Kline. *Mathematics – The Loss of Certainty*. Oxford University Press, New York, 1980.

9) Joan L. Richards: "The Art and the Science of British Algebra: A Study in the Perception of Mathematical Truth". *Historia Mathematica*,Vol. 7, 1980, pp. 343-365.
Harvey W. Becher: "Woodhouse, Babbage, Peacock, and Modern Algebra". *Historia Mathematica*, Vol. 7, 1980, pp. 389-400.
Harvey W. Becher: "William Whewell and Cambridge Mathematics". *HSPS*, Vol. 11, No. 1, 1980, pp. 1-48.
Helena M. Pycior: "George Peacock and the British Origins of Symbolical Algebra". *Historia Mathematica*, Vol. 8, 1981, pp. 23-45.

10) See for example the following translations from German:
W. Gellert, H. Küstner, M. Hellwich & H. Kästner (eds.). *The VNR Concise Encyclopedia of Mathematics*. Van Nostrand Reinhold Co., New York, 1977.
Friedrich Waismann: *Introduction to Mathematical Thinking – The Formation of Concepts in Modern Mathematics*. Harper Torch Books, New York, 1959.

11) O. I. Franksen: "The Virtual Work Principle – A Unifying Systems Concept". In Ø. Bjørke & O. I. Franksen: *Structures and Operations in Engineering and Management Systems*. Tapir Publishers, Trondheim, Norway, 1981, pp. 17-152.

12) BL, Add. Ms. 37202, F. 125.

13) O.I. Franksen: "An Operational Formulation (in APL) of the Electric Network Problem". In Ø. Bjørke & O. I. Franksen: *System Structures in Engineering – Economic*

Design and Production. Tapir Publishers, Trondheim, Norway, 1978, pp. 15-178.

14) *Journal of the Royal Institution of Great Britain*, Vol. 3, 1817, pp. 72-77 & Plate II.

15) Dubbey actually used the term a *Latin square*, but that must be a slip of the tongue. A Latin square is an arrangement of n distinct symbols in a square of size n^2, such that each symbol occurs once in every row and every column. In other words, each row and each column is a permutation of the n distinct symbols. The notion was introduced by Euler as a new species of magic squares, in an extensive memoir he wrote a few years before his death in 1783. The modern term "Latin" derives from the fact that in this memoir Euler used Latin letters as his symbols. See for example, H. Howard Frisinger: "The Solution of a Famous Two-Centuries-Old Problem: The Leonhard Euler Latin Square Conjecture", *Historia Mathematica*, Vol. 8, 1981, pp. 56-60.

16) I am indebted to Mr. Svein Molaug, the director of Norsk Sjøfartsmuseum, for permission to reproduce this drawing, which he made immediately after the ruler was recovered. Also carved into the ruler is what looks like an inscription of 22 letters. Since three letters: ILV are twice repeated, while three vowels: E O Y and four consonants: DGJP are missing, it is perhaps an *anagram*. That is, a more or less arbitrary reordering or permutation of the letters of a name or meaningful sentence. Another possibility is a navigational code related, say, to map-reading.

17) Paul S. Herwitz: "The Theory of Numbers". In Morris Kline (ed.): *Mathematics in the Modern World*. W. H. Freeman & Co., San Francisco, 1968, pp. 98-101.

18) Gene McDonnell: "Magic Squares and Permutations", *APL Quote Quad*, Vol. 7, Issue 3, 1976, pp. 25-28. This article gives an algorithm, attributed to Ray Polivka, which is unusual by being non-iterative. The construction of a magic square in the APL Terminal Session of this part, is based on this algorithm.

19) Helen Fouché Gaines: *Elementary Cryptanalysis*, 1939. Reprinted under the new title *Cryptanalysis – A Study of Ciphers and Their Solution*, Dover Publications, Inc., New York, 1956.

20) *Op cit.*, note 31, part 1.

21) Carl Friedrich Gauss: *Werke*, Vol. 5. Göttingen, 1867.

22) Morris Kline: *Mathematical Thought from Ancient to Modern Times*. Oxford University Press, New York, 1972.

23) BL, Add Ms. 37205: "Scientific Papers of Charles Babbage. 2. Mathematical recreations and investigations of the laws of tit-tat-to, etc.; 3. Febr. 1825 – 18. April 1865"; FF. 304-384.

24) Quoted by F. Cajori: *A History of Mathematical Notations*. Vol. II: *Notations Mainly in Higher Mathematics*. The Open Court Publishing Company, Chicago, Illinois, 1929. Reprinted 1952.

25) Gabriel Kron. *Tensor Analysis of Networks*. John Wiley & Sons, Inc., New York, 1939. Reprinted by MacDonald & Co., Ltd., London, 1965.

26) Léon Brillouin: *Tensors in Mechanics and Elasticity*. Academic Press, New York, 1964 (Translation of the French edition from 1938).

27) Karl Menninger: *Number Words and Number Symbols. A Cultural History of Numbers*. The M.I.T. Press, Cambridge, Massachusetts, 1967.

28) John Maynard Keynes: "Newton, the Man". Reprinted in James R. Newman (ed.): *The World of Mathematics*, Vol. 1, Simon & Schuster, New York, 1956, pp. 277-285.

29) Sven B. F. Jansson: *Runinskrifter i Sverige*. AWE/GEBERS, Uppsala, 1977. Lise Lotte Nielsen: "Jysk fund – runer ristet i sølv". Berlingske Tidende, 6 (IV), 18. december 1983. Ongoing excavations of the sacrifices of war booty from about 200 A.D. in the Illerup River Valley near Skanderborg in Denmark, in the summer of 1983 brought to light hitherto unknown forms of the runic letters *(th)* and *w*. See also the following two articles. Jørgen Ilkjær and Jørn Lønstrup. "Runefundene fra Illerup Ådal. En arkæologisk vurdering af vore ældste runeindskrifter", and Erik Moltke and Marie Stoklund: "Runeindskrifterne fra Illerup mose", *KUML 1981, Årbog for Jysk Arkæologisk Selskab*. I kommission hos Gyldendals Boghandel, Nordisk Forlag, København 1982, pp. 49-65 and 67-79. The latter two articles contain extensive summaries in English.

30) John R. Clark Hall: *A Concise Anglo-Saxon Dictionary*, Cambridge at the University Press, 1814. Reprinted 1975.
The meaning of the Anglo-Saxon word *æht* is possession, ownership, or control. It was derived from *āgan* (to own), meaning "those which belong to" or "belong together". The related word in old English is *aught* for "ever a thing" or "anything", and in modern English it is the substantive *aught* (e.g., "for aught we know..."). In Danish the word *æt* is an archaic term for the word "kin".

31) Niels W. Bruun and Allan A. Lund. *Tacitus Germania*, Vols. I and II, Wormianum, Århus, 1974.

32) *Nordens Gudekvad*. På dansk ved Thøger Larsen, 1926-27. Reprinted in Gyldendals Trane-Klassikere, København, 1968.

33) Aslak Liestøl: "Jeg rister bodruner, jeg rister bjærgeruner". *Skalk*, Nr. 5, 1964, pp. 18-27, (or "Runer frå Bryggen", *Viking*, Bd. XXVII, Oslo 1964). See also the many references in Else Roesdahl: *Danmarks Vikingetid*, Gyldendal, København, 1980.

34) The rather widespread ability to read and write runes is reflected in our modern languages. For example, to "scratch" runes is *riste runer* in Danish. The modern form of the verb is *ridse*, which literally is to "scratch" but in certain connotations also has the meaning of "sketch or outline" as in *grundrids*, that is a line drawing. In modern Swedish it became *rita*, meaning "to draw". In Anglo-Saxon, preserving on initial letter *W-* which disappered early (600-800 A.D.) in Scandinavian pronunciation, it was

writan, and hence, in modern English *write*. It is interesting to note in this connection that English did not adopt the Latin word *scribere* for "writing", as it was done in the Scandinavian languages (Danish, *skrive*), influenced by the Church. The word *rune* means "secret" or "council". In the latter sense, it is recognized in the name *Runnymede* or "council meadow", the site on the Thames west of London where King John signed the Magna Charta in 1215. A fascinating account of the Danish influence on the English language is given in, Torben Kisbye: *Vikingerne i England – sproglige spor*. Akademisk Forlag, København, 1982

35) Else Roesdahl, *op.cit.* (See note 33). See also Olaf Olsen, *Fyrkat*, Nationalmuseet, 5. rev udg., København 1982. I am grateful to Dr. Olaf Olsen, keeper of National Antiquities, Nationalmuseet, Copenhagen, for permission to reproduce from this book the layouts of the four ring fortresses from the Viking Period, shown in figure 13.

36) Lis Jacobsen and Erik Moltke: *Danmarks Runeindskrifter*, København, 1942

37) I. B. Lindenfels, *op.cit.*, (note 19, part 1)

38) Louis Trenchard More, *op.cit.*, (note 36, part 1).

39) The photographies of the three cipher runes, excavated on Bryggen in Bergen, were made by the late Mr. A. Liestøl, a well-known Norwegian authority on runic inscriptions. They are reproduced here by permission of the copyright owner, Universitetets Oldsaksamling in Oslo. I am grateful to Kjersti Markali, Oldsaksamlingen, for supplying me with detailed and precise information on the reading and interpretation of these ciphers

40) BL, Add Ms. 37205, F. 17

41) Harvey W. Becher, *op cit.*, (note 9).

42) Anthony Hyman, *op cit.*, (note 4, part 1)

43) C. C. Bombaugh: *Gleanings for the Curious*, 1890. Reprinted under the title: *Oddities and Curiosities of Words and Literature*, Dover Publications, Inc., New York, 1961

44) Velma R. Huskey & Harry D. Huskey: "Lady Lovelace and Charles Babbage". *Annals of the History of Computing*, Vol. 2, No. 4, Oct. 1980, pp. 299-329.

45) Babbage's association with Boole and other British mathematicians is recounted by Hyman, *op.cit.* (note 4, part 1). A discussion of Menebrea's paper and its annotated translation by Lady Lovelace is given in my article, cited earlier (note 5, part 1)

46) Thomas L. Hankins, *Jean d'Alembert – Science and the Enlightment*. Clarendon Press, Oxford, 1970. Lindenfels, *op.cit.* (note 19, part 1), gives the reference to d'Alembert as "*Encyclopédie méthodique, Grammaire & Littérature, Tome I, p. 545*"

47) D. Kahn, *op.cit.* (note 25, part 1), apparently suggests that the letters are written on the center of the strip, because he says that "*the disconnected letters make no sense unless the parchment is rewrapped ... then words leap from loop to loop, forming the message*" (page 82). Further, considering the contributions to cryptography by Edgar Allan Poe, he says: "*Poe here gave cryptography its first discussion of skytale cryptanalysis. Wrap the strip of parchment around a cone and slide it up and down until sense appears, the diameter of the cone at that point is the diameter of the skytale*" (page 788)

48) Norman L. Biggs, E. Keith Lloyd & Robin J. Wilson: *Graph Theory 1736 – 1936*. Clarendon Press, Oxford 1976

49) I. M. Copilowish: "Matrix Development of the Calculus of Relations", *Journal of Symbolic Logic*, Vol. 13, No. 4, 1948, pp. 193-203. R. D. Luce: "A Note on Boolean Matrix Theory", *Proc. Am. Math. Soc.*, Vol. 3, 1952 pp. 382-388. F. I. Mautner: "An Extension of Klein's Erlanger Program: Logic as an Invariant Theory", *Am. J. Math.*, Vol. 68, 1946, pp. 345-384

50) F. Klein: *Vergleichende Betrachtungen über neuere geometrische Forschungen*, Verlag von Andreas Deichert, Erlangen, 1872 (reprinted 1982 by Math. Inst. Univ. Erlangen-Nürnberg). Rev. ed. published by F. Klein in *Math. Ann.*, Bd. 43, 1893, pp. 63-100.

51) O. I. Franksen, *op. cit.*, (note 43, part 1).

52) T. More. "Notes on the Diagrams, Logic, and Operations of Array Theory", In Ø. Bjørke & O. I. Franksen: *Structures and Operations in Engineering and Management Systems*. Tapir Publishers, Trondheim, Norway, 1981, pp. 497-666. Contains an extensive bibliography on Array Theory

53) C. F. Bricka (ed.). *Dansk Biografisk Lexicon*, Bd. XIII, København, 1899, pp. 60-63. Or, Povl Engelstoft (ed.): *Dansk Biografisk Leksikon*, Bd. XVIII, København, 1940, pp 226-228. See also, C. A. Schou & T. Vogel-Jørgensen (eds.): *Illustreret Dansk Konversations Leksikon*, Bd. 17, Berlingske Forlag, København 1936, pp. 91-92.

54) O. I. Franksen, P. Falster & F. J. Evans: *Qualitative Aspects of Large Scale Systems – Developing Design Rules Using APL*. Lecture Notes in Control and Information Sciences, Vol. 17, Springer-Verlag, Berlin, Heidelberg, New York, 1979.

55) Julius Petersen: *Système Cryptographique*. Imprimerie de C. Ferslew & Co., Copenhague, 1875. 15 pages.
Petersen closes this "*notice*" (or note), as he calls it, dating it "*November 1875*". Since no references are given to the effect that it is a reprint of an earlier publication, it seems reasonable to assume that this is the original issue. I have not investigated whether it appeared later on in one of the many journals to which he contributed.

56) I am grateful to Lt. Col. W. L. Christensen, the Danish Army Librarian, and his staff for their time and effort doing research for me on this question in the Army Archives

57) Kahn, *op. cit.* (note 25, part 1), and Gaines, *op.cit.* (note 19).

58) Herbert Meschkowski. *Wandlungen des mathematischen Denkens.* Friedr. Vieweg & Sohn, Braunschweig, 1964.

59) Herbert Meschkowski. *Ways of thought of great mathematicians.* Holden-Day, Inc., San Francisco, London, Amsterdam, 1964.

60) C. A. Schou & T. Vogel-Jørgensen, *op.cit.* (note 20, part 1), Bd. 10, pp. 305-306.

61) Kenneth E. Iverson: *A Programming Language.* John Wiley & Sons, New York, 1962.

62) Sometime after I had formulated this basic identity from purely abstract geometrical considerations, my attention was called to the fact that Professor M. A. Jenkins at the Computing and Information Science Department, Queen's University in Canada, had described it prior to me in a technical university report *"On combining the Data Structure Concepts of Lisp and APL"* (No. 80-109, Sept. 1980, 13 pages). As subsequent discussions revealed during Professor Jenkins' visit with my department in May 1984 he attached no less significance than I did to this identity. This we both found quite remarkable considering that we had arrived at the statement independent of each other and by so totally different reasoning.

63) O. I. Franksen, *op.cit.* (note 5, part 1).

64) See the VNR *Concise Encyclopedia* (note 10).

65) Abraham Pais: *Subtle is the Lord ..., The Science and the Life of Albert Einstein.* Clarendon Press, Oxford; Oxford University Press, New York, 1982, pp. 274-276.

66) O. I. Franksen & Ø. Bjørke: "Datamatic Baseoperations in Factory Management Systems". *Computers in Industry,* Vol. 1, 1980, pp. 289-295.

67) I am grateful to Dr. H. Weinert, executive editor of *Systems Analysis, Modeling, and Simulation,* Akademie der Wissenschaften der DDR, for clarifying this point about German grammar.

68) Of the many delightful books on symmetry, two are truly classic. One is by the famous mathematician and contributor to the philosophy of science, Hermann Weyl: *Symmetry,* Princeton University Press, Princeton, New Jersey, 1952. The other is a BBC television transcript from 1965 of a series of lectures by the brilliant educator and Nobel Prize winner in physics, Richard P. Feynman: *The Character of Physical Law,* The M.I.T. Press, Cambridge, Massachusetts, 1967. A typical exposition for the graduate student working towards a professional career, may be J. P. Elliott & P. G. Dawber *Symmetry in Physics,* Vols. 1 & 2. The Macmillan Press, Ltd., London, 1979.

69) A. Cayley. "On the Theory of Groups, as Depending on the Symbolic Equation $\Theta^n = 1$", Parts I & II. *The Philosophical Magazine and Journal of Science,* Vol. VII, Fourth Series, No. XLII, Jan. 1854, pp. 40-47 & No. XLVII, June 1854, pp. 408-409.

70) Lewis Carroll: *Alice in Wonderland.* J. M. Dent & Sons, Ltd., London, 1961.

71) The technical literature in this area is often difficult to comprehend for the modern student because of its assumptions on prerequisite knowledge. A remarkable and brilliant introduction to the necessary mathematics of invariant theory is, Daniel Edwin Rutherford: *Substitutional Analysis,* Edinburgh at the University Press, 1940. In this book which appears to be rather little known, Rutherford gives a splendid account of the works of Alfred Young, whose results on the reduction of the symmetric group to irreducible representations and the presentation of these representations in an explicit form, the so-called "Young diagrams", have turned out to be of central importance in modern physics and chemistry. Rutherford recounts that Young published his researches in the period from 1900 to 1935. Between his second paper in 1902 and his third in 1927 there is a gap of twenty-five years. This is due to the fact that Young was not a professional mathematician but a country clergyman with numerous clerical duties. Also, in this period Young undertook a study of the German language to enable him to assimilate the papers of the German mathematicians, Schur and Frobenius, which made a great impression on him and spurred him on to develop his own approach to the subject.

72) Julius Petersen: *De algebraiske Ligningers Theori.* Andr. Fred. Høst & Søns Forlag, Kjøbenhavn 1877.

73) O. I. Franksen: "Testing Group Axioms". *APL Quote Quad,* Vol. 13, No. 2, December 1982, pp. 11-12.

74) It is impossible to do justice to the many splendid books which have appeared in our time on groups and algebraic structures. Instead, I shall confine myself to four books, selected to illustrate each an entirely different pedagogical angle on this topic area. They are all very good introductions, starting from scratch and with excellent and illustrative examples. An authoritative approach along more traditional lines is, Walter Ledermann: *Introduction to the Theory of Finite Groups;* Oliver and Boyd, Edinburgh and London, Fourth Revised Edition, 1961. A geometrical approach, emphasizing the patterns of the multiplication table and depicting groups by digraphs, is, Israel Grossman and Wilhelm Magnus: *Groups and Their Graphs,* Random House New Mathematical Library, The L. W. Singer Company, U.S.A., 1964. A book for helping and inspiring the mathematics teacher is, D. E. Mansfield and M. Bruckheimer: *Background to Set and Group Theory;* Chatto and Windus, Ltd., London, 1971. A work of sheer love for the art of mathematics, taking the reader on a tour through such inspiring and unusual applications of group theory as that of bell-ringing, is, F. J. Budden: *The Fascination of Groups,* Cambridge University Press, Cambridge, 1978.

75) The APL formulation I have adapted here for the associative law, seems to originate with, A. D. Falkoff and K. E. Iverson: "The APL\360 Terminal System", *IBM Research Report,* No. RC-1922, 16 Oct. 1967, pp. 1-20.

76) Usually quoted from Cervantes' *Don Quixote*, the sentence has been traced back to antique Greece by, T. Vogel Jørgensen: *Bevingede Ord*, Tredie reviderede Udgave, G. E. C. Gads Forlag, København, 1948. I am grateful to Mrs. Norsbo for supplying me with the English translation.

77) P. W. Bridgman: *On the Nature of Physical Theory*, 1936. Reprinted by Dover Publications, Inc., New York. P. W. Bridgman: *The Way Things Are*, 1959. Reprinted by the Viking Press, New York, 1961

78) Colin Cherry: *On Human Communication*, John Wiley & Sons, Inc., New York, 1957. Translated into German under the title: *Kommunikationsforschung – eine neue Wissenschaft*, S. Fischer Verlag, Hamburg, 1964

79) In addition to the references in notes 11 and 13, the reader may wish to consult my paper "Mathematical Programming in Economics by Physical Analogies", Part I-III, *Simulation*, 1969; No. 6, pp. 297-314, No. 1, pp. 25-48; No. 2, pp. 65-87. Or, my article "Basic Concepts in Engineering and Economics", in J. J. van Dixhoorn & F. J. Evans (eds.): *Physical Structure in Systems Theory – Network Approaches to Engineering and Economics*, Academic Press, London, 1974, pp. 247-278

80) Norman R. Campbell: *Physics, The Elements*, 1919. Reprinted under the title: *Foundations of Science. The Philosophy of Theory and Experiment*, by Dover Publications, Inc., New York, 1957. Norman R. Campbell, *What is Science?*, 1921. Reprinted by Dover Publications, Inc., New York.
S. S. Stevens, "On the Theory of Scales of Measurement", *Science*, Vol. 103, No. 2684, June, 1946, pp. 677-680. S. S. Stevens: "Measurement, Psychophysics, and Utility". In C. West Churchman & Philburn Ratoosh (eds.): *Measurement – Definitions and Theories*, John Wiley & Sons, Inc., New York, 1959, pp. 18-64.

81) In the early sixties, I was privileged to visit with Professor Stevens at Harvard a couple of times. Prior to that, Gabriel Kron and others had preached me on the vital importance of "invariance under a group of transformations". Yet, it surprised me to hear the same thing from a man who was so evidently preoccupied with the psychological behaviour of man as Professor Stevens, when I accidentally triggered him. I think he called it "the lesson of physics", although I am pretty certain that he did not mention the Erlanger Program.

82) G. D. Birkhoff: *Dynamical Systems*, American Mathematical Society Colloquium Publications, Vol. IX, Providence, Rhode Island, 1927. Reprinted 1966

83) John von Neumann and Oskar Morgenstern: *Theory of Games and Economic Behaviour*, 1944. Science Editions, John Wiley & Sons, Inc., New York, 1964

84) Karl Raimund Popper: *The Logic of Scientific Discovery*, Hutchinson & Co., Ltd., London, 1959. Revised edition, 1972.

85) Gabriel Kron: *The Application of Tensors to the Analysis of Rotating Electrical Machinery*, General Electric Review, Schenectady, New York, 1938. Second enlarged edition, 1942. Gabriel Kron: *op.cit.*, note 25. Gabriel Kron: *A Short Course in Tensor Analysis for Electrical Engineers*, 1942. Reprinted under the title: *Tensors for Circuits*, Dover Publications, Inc., New York, 1959.

86) Morrison & Morrison, *op.cit.* note 3, part 1.

87) Trenchard More: *op.cit.*, note 52.

88) To test and improve the applicability of Array Theory in a computational environment, the theory has formed the basis for the implementation of experimental programming languages, first by IBM, and later jointly by IBM and Professor M. Jenkins at Queen's University in Canada. The latter language, developed with "C" as host language, is called *NIAL (Nested Interactive Array Language)* after the Old Norse Nial's Saga. Not commercially available, it is presently tested at different universities in USA, Canada, England, and the Scandinavian countries. The Electric Power Engineering Department of the Technical University of Denmark is one of these "test sites". In a joint venture with Danish Industry, our aim is to explore the potential of Array Theory and NIAL in real-life applications. My colleagues, our doctoral students, and I are all indebted to Dr. More and Professor Jenkins for their interest and unfailing support and cooperation in this project.

89) Karl Fritz Ruehr: "A Survey of Extensions to APL", *APL Quote Quad*, Vol. 13, No. 1, 1982, pp. 277-314

90) Trenchard More, Jr.: "An Interactive Method for Algebraic Proofs". *IBM Philadelphia Scientific Center*, Technical Report No. 320-3005, Sept. 1971, 89 pages. An invited address to the 25th Summer Meeting of the Canadian Mathematical Congress, the paper discusses experimental investigations of multiplication tables which, conducted interactively in APL, lead to detailed proofs of theorems on groups, semigroups, and lattices.

91) Trenchard More, Jr.: "On the Composition of Array-Theoretic Operations". *IBM Cambridge Scientific Center*, Technical Report No. 320-2113, May 1976, 52 pages. A privately circulated appendix of 108 pages to this report, entitled "A Table of Array-Theoretic Operations", provides a documentation of the entire multiplication table of some 250 operations.

92) Abraham A. Fraenkel: *Abstract Set Theory*, First edition, North-Holland Publishing Company, Amsterdam, 1953.

93) A. D. Falkoff & K. E. Iverson: *APL\360: User's Manual*. IBM Thomas J. Watson Research Center, U.S.A., August 1968.

94) As I recall the explanation given to me by Dr. Kenneth Iverson some years ago during a visit in Copenhagen, he and the other designers of APL were compelled to make this

choice of notation for the permutational transposition even if, originally, they endeavoured to keep the correct algebraic form. The reason for this was that, alternatively, they had to give up using the same notation for the repeated-index transposition

95) J. L. Synge & A. Schild. *Tensor Calculus*. University of Toronto Press, Toronto, 1949. Reprinted with corrections, 1962.

96) E. E. McDonnell: "Sauce for the gander (or adding a vector to a matrix)", *APL Quote Quad*, Vol. 9, No. 3, 1979, pp. 64-66.

97) Richard Bellman: *Introduction to Matrix Analysis*. McGraw-Hill, Inc., New York, 1960.

98) Birger Trolle. "Louis Pasteur. Hans vej fra kemien til mikrobiologien". *Brygmesteren*, No. 8, 1962, pp. 195-210.

99) Erich Worbs. *Carl Friedrich Gauss – Ein Lebensbild*. Koehler & Amelang, Leipzig, 1955. Another famous name on the reproduction of this page of signatures, is that of Ørsted's Swedish friend, the chemist Jac. Berzelius.

100) O. I. Franksen: "Group Representation of Finite Polyvalent Logic – A Case Study Using APL Notation". In A. Niemi (ed.): *A Link Between Science and Applications of Automatic Control – IFAC VII World Congress*. Pergamon Press, Oxford and New York, 1979, pp. 875-887.

101) Max Planck: *Wissenschaftliche Selbstbiographie – Mit der von Max von Laue gehaltenen Traueransprache*. 3. Auflage, Johann Ambrosius Barth Verlag, Leipzig, 1955.

A Conservation Law of the Message

1) Lindenfels, *op.cit.* (note 19, part 1)

2) Babbage, *op.cit.* (note 11, part 1)

3) Hyman, *op.cit.* (note 4, part 1)

4) L. H. Dudley Buxton. "Charles Babbage and his Difference Engine", *Transactions of the Newcomen Society*, Vol. XIV, 1933-34, pp. 43-46. Inquiries about these dictionaries to a number of British museums have been in vain. Likewise, Mr. Gary Tee's investigations in New Zealand and Australia have been negative (see note 1, part 1). Still, I am indebted to Mr. Tee for his unfailing support in this matter.

5) Babbage, *op.cit.* (note 3, part 1)

6) A typical illustration of a pre-computer publication of linguistic material, including pattern words and trigrams, is found in, Fletcher Pratt: *Secret and Urgent – the Story of Codes and Ciphers*, Robert Hale, Ltd., London, 1923. It may be contrasted with the 212 pages of non-pattern words found in, Wayne G. Barker: *Cryptanalysis of the Simple Substitution Cipher with Word Divisions, Using Non-Pattern Word Lists*, Aegean Park Press, Laguna Hills, California, 1975. Produced by computer, this list of non-pattern words is ordered by word lengths or number of letters; for each word length by the vowel-consonant pattern; and lexicographically within each such pattern. The use of non-pattern words provides an interesting dual or symmetry to that of pattern words.

7) Some very instructive approaches, combining letter frequency counts with the search for vowel-consonant patterns, are given in, Helen Fouché Gaines, *op.cit.* (note 19, part 2), and William F. Friedman: *Elements of Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1976. The latter book is a reprint of Friedman's now classic textbook for the U.S. Signal Corps, issued by the Chief Signal Officer in May 1923 as Training Pamphlet No. 3. It was by the title of this book that Friedman promoted his coinage of the word "*cryptanalysis*", meaning the unauthorized deciphering of cryptograms. Although quite popular in the U.S.A., the term has not gained foothold in Europe with its century-old literary background and its strong French influence on terminology.

8) Quoted by Cajori, *op.cit.* (note 7, part 2).

9) The references to the two biographies, published anonymously by Fourier, are given in the authoritative work by, I. Grattan-Guinness & J. R. Ravetz: *Joseph Fourier, 1768-1830*, The MIT Press, Cambridge, Mass., 1972. The two references are: "François Viète", *Biographie universelle ancienne et moderne*, tome 48, Paris, 1827, pp. 444-447. Nouvelle Édition, tome 43, pp. 361-363. "Jean Wallis", *ibid.*, tome 50, Paris, 1827, pp. 130-134. Nouvelle Édition, tome 44, pp. 283-284.

10) C. Babbage: "Sur l'emploi plus ou moins fréquent des mêmes lettres dans les différentes langues". *Correspondance mathématique et physique*, tome 7, 1831, pp. 135-137 (See also, BL.Add.Ms. 37205, F. 230). For bibliographical information see, A. W. Van Sinderen, *op.cit.* (note 1, part 1).

11) I am grateful to Mrs. E. Norsbo for this information.

12) Kahn, *op.cit.* (note 25, part 1).

13) Solomon Kullback: *Statistical Methods in Cryptanalysis*, Aegean Park Press, Laguna Hills, California, 1976. Reprint with added problems of the original edition from 1935.

14) Since we are concerned with chance phenomena having only a finite number of possible outcomes, the necessary mathematics can be brought down to the level of secondary schools such as described in, *Introductory Probability and Statistical Inference for Secondary Schools*, – an experimental course prepared for the Commission on Mathematics, College Entrance Examination Board, New York, 1957.
Like we are concerned with a situation of statistical independence in the phitest, so we may consider cryptographical techniques based on conditional probabilities. Here, a very instructive case is the iterative solution of a monoalphabetically enciphered cryptogram by consideration of the frequency of occurrence of diagrams or trigrams.

The theory is given in, Shmuel Peleg: "A New Probabilistic Relaxation Scheme", *IEEE Conference on Pattern Recognition and Image Processing*, Chicago, 1979, pp. 337-343; and Shmuel Peleg & Azriel Rosenfeld: "Breaking Substitution Ciphers Using a Relaxation Algorithm", *ACM Communications*, Vol. 22, No. 11, 1979, pp. 598-605. Reformulated into multidimensional APL arrays, the model becomes quite simple and can be stated in about fifteen APL statements with the iteration function itself requiring about five statements. However, the memory requirement significantly exceeds the 64 K, arbitrarily set as the limit in all our other applications.
From a pedagogical point of view, this cryptographical model may be derived by simple means from the well known theorem, published in 1763 by the Reverend Thomas Bayes, one of the founding fathers of the Royal Society. Modern Bayesian analysis is difficult to teach, because it requires intimate knowledge of the field of application to establish the a priori probability distribution prerequisite to the analysis. This problem is overcome quite easily here. Also, the model provides convincing illustrations of the dependence upon this a priori evidence (as compared with the sample evidence), as well as upon symmetries caused, for example, by a reciprocal alphabet.
I am indebted to Mr. Gert Møller, graduate student, for carrying out these investigations of the model, the APL formulation of which I merely sketched for him.

15) Charles J. Mendelsohn: "Blaise de Vigenère and the Chiffre Carré", *Proceedings of the American Philosophical Society*, Vol. 82, No. 2, 1940, pp. 103-129.

16) Biographical information about Lindenfels is published in, D. L. Lübker & W. Schröder (eds.): *Lexicon der Schleswig-Holstein-Lauenburgischen und Eutinischen Schriftsteller von 1796 bis 1828*, Erste Abteilung A-M, Altona, 1829, pp. 347-350. R. Nyerup et. al.: *Alm. Litteraturlexicon*, Kjøbenhavn, 1820, pp. 346-347. Ths. Hansen Erslew: *Alm. Forfatter-Lexicon*, Bd. 2, Kjøbenhavn 1847, pp. 151-153. C. F. Bricka: *Dansk Biografisk Lexikon*, Bd. X, Kjøbenhavn, 1896, page 314.
The latter three are incorrect as far as pertains Lindenfels' military service in France prior to his arrival in Denmark. The correct data, which confirm the information given by Lübker and Schröder, are to be found in the Danish Army Archives: *Conduiteliste for D'Hr. Officerer af det Kongelige Artillerie Corps danske Bataillon*, Kjøbenhavn, 29. Sept. 1814; and V. Richter: *Den danske Landmilitæretat*, 2. del, Kjøbenhavn 1897, page 39 (handwritten). I have also been supplied with a copy of another handwritten page which appears to be part of a bibliographical list of all Officers in the Danish Army.
I am grateful to the Army Librarian, Lt.Col. W. L. Christensen, and his staff for their ready and indispensable help in establishing the historical facts about Lindenfels and his military background.

17) The explanation of the motto: "*Et blot til Lyst*", adopted by Lindenfels for his book, is given by T. Vogel-Jørgensen, *op.cit.* (note 76, part 2).

18) Jens Johansen, *op.cit.* (note 22, part 1). Also by the same author, *Krigen 1848-49-50; Kortfattet historisk fremstilling og befæstningsanlæg*. Særtryk af Tøjhusmuseets bog om Treårskrigen 1848-49-50, Bd. I., N. Olaf Møllers Bogtrykkeri, København 1948, pp. 11-126.
These two references by my late grandfather, the war-historian and army archivarian, Lt. Col. Jens Johansen, were written in my boyhood, so I have many fond recollections of his telling me about his research. In particular, I remember his enthusiasm when in the army archives he found the fatal dispatch which, stopping the advance of the Third Brigade at the battle of Isted 1850, prevented a decisive Danish victory. This, he claimed (both to me and in his last-mentioned reference), permitted the insurgent army to get away intact, thereby laying the military foundation for Bismarck's "excuse" to attack Denmark in 1864, with the subsequent unhappy events for the country. The dispatch, which is reproduced in his book, is in plaintext; and, as I think back, I have the distinct impression that he took it for granted that dispatches of the day were never enciphered.

19) Mathilde Ørsted: *Breve fra og til Hans Christian Ørsted*, Første Samling. Th. Linds Forlag, Kjøbenhavn, 1870.

20) "A New Cipher Code", *Scientific American Supplement*, No. 2143, Vol. 83, page 61.

21) G.P.B.: "Ciphers and Cipher-Writing", *op.cit.* (note 31, part 1).

22) M.W. Bowers (pseud. Zembie): "Major F. W. Kasiski – Cryptologist". *The Cryptogram*, Vol. XXXI, No. 3, Jan.-Feb. 1964, pp. 53, 58-59.

23) BL., Add.Ms. 37205, FF. 43-65.

24) Kahn reproduces folio 249 with the third formulation on page 206 of his book (*op.cit.*, note 25, part 1), but he does not comment on the meaning of the equation or its importance.

25) It is well-known from Babbage's description in his first anonymous letter to the Royal Society of Arts, Sept. 1st, 1854, that he owned various mechanical cipher aids: slides, discs, and a box-wood cylinder. Apparently, none of these contraptions have survived, apart from some simple paper strips among his papers in the British Library. L.H. Dudley Buxton, (*op.cit.*, note 4), stated in 1933 that Babbage "*constructed a curious machine in which you wrote words or symbols on wooden cubes and turned the handle. This machine is in my possession, but I do not know how it was intended to work*". In the hope that it was one of Babbage's cipher aids, I traced this machine to the Oxford University Museum of the History of Science, in the old Ashmolean Building. Known as the "*Metabolical Machine*", it was patented by one Alfred Lang in 1864. However, rather than being a cipher aid, it turned out to be a "*Means or Apparatus to Facilitate the Acquisition of Languages, and Applicable also in Producing Various Changes in Musical Combinations*". I am indebted to the Curator, Mr. Francis Maddison, and to Miss Elizabeth M. Buxton for invaluable help and assistance in this search.

26) Morris Kline, *op.cit.* (note 22, part 2).

27) A.G. Keller: "Joan Gadol, Leon Battista Alberti: Universal Man of the Renaissance", *Technology and Culture*, Vol. 12, No. 4, October, 1971, pp. 632-635.

28) BL, Add.Ms. 37205, F. 13.

29) BL, Add.Ms. 37205, FF. 4-11 (worksheets); FF. 268-269 (cypher No. 1 partly solved); FF. 271-272 (key to cypher No. 2).

30) BL, Add.Ms. 37205, FF. 63-65.

31) De Viaris: "Cryptographie", *Le Génie Civil*, tome XIII, 1888, pp. 24-27, 38-39, 55-56, 72-75, 84-88 & 104-107. See, in particular, the first two articles.

32) In April 1972, unaware of de Viaris' contribution, I rediscovered his cryptographic equation. In turn, this led me to the formulation of the "missing" cipher, which I have called Vigenère's Variant in this account. From the very first, I was inspired by the obvious analogy to the energy conservation law; and the rest really followed by simple considerations of symmetry. I imagine, perhaps fancifully, that de Viaris followed a similar path.

33) See part IV of my paper: "Are Data-Structures Geometrical Objects?" (*op.cit.*, note 43, part I) concerning an extension of these ideas to a group-theoretical formulation in APL of Boolean operations. A further generalization to many-valued logics may be found in my paper: "Group Representation of Finite Polyvalent Logic – a case study using APL notation"; *IFAC VII World Congress*, Helsinki, June 1978. Reprinted in A. Niemi: *A Link Between Science and Applications of Automatic Control;* Pergamon Press, Oxford & New York, Vol. 2, 1979, pp. 875-887. All mathematics in the latter paper is formulated in terms of APL statements, so that by entering these statements on the terminal, the reader is able immediately to experiment with the approach.

34) The public exchange of letters between Babbage and Thwaites in the *Journal of the Society of Arts* for 1854, is reproduced here by permission of the Society (see note 8, part 1). The letters appear in Vol. II, 1854, in the following order:
1. J.H.B. Thwaites: "Secret, or Cypher Writing", No. 90, Aug. 11, pp. 663-664.
2. C. [Babbage]: "Mr. Thwaites's Cypher", No. 93, Sept. 1, pp. 707-708.
3. J.H.B. Thwaites: "Secret, or Cypher Writing", No. 95, Sept. 15, pp. 732-733.
4. C. [Babbage]: "Mr. Thwaites's Cypher", No. 98, Oct. 2, pp. 776-777.
5. J.H.B. Thwaites: "Mr. Thwaites's Cypher", No. 99, Oct. 13, page 791.
6. J.B. Kearney: "Mr. Thwaites's Cypher", No. 100, Oct. 20, pp. 803-804.

35) W.D. Niven (ed.): *The Scientific Papers of James Clerk Maxwell*, Vols. I & II, Cambridge University Press, 1890. Reprinted by Dover Publications, New York, 1965.

36) I am indebted to Professor Bryan Thwaites, Brigadier P.T. Thwaites, and Mr. B. St.G. Thwaites for their kind responses to my inquiries. The latter even provided me

with information from the Bristol Directory for the years 1850-70, which he consulted during a visit "*with a few minutes to spare*". Thus, he found that his namesake was listed as "*surgeon, dentist*", and that he moved from 17 Park Street soon after 1854 to 2 Dover Place, Clifton. Further, since his name was not listed after 1865, we may assume that he either died or moved away.

37) Mr. Garry J. Tee kindly searched this index for me.

38) I am grateful to Mr. D.J. Bryden, Assistant Keeper, Pictorial and Archive Collection, Science Museum Library, London, for supplying me with a copy of Thwaites' printed provisional specification, No. 1727, A.D. 1854, 3 pages.

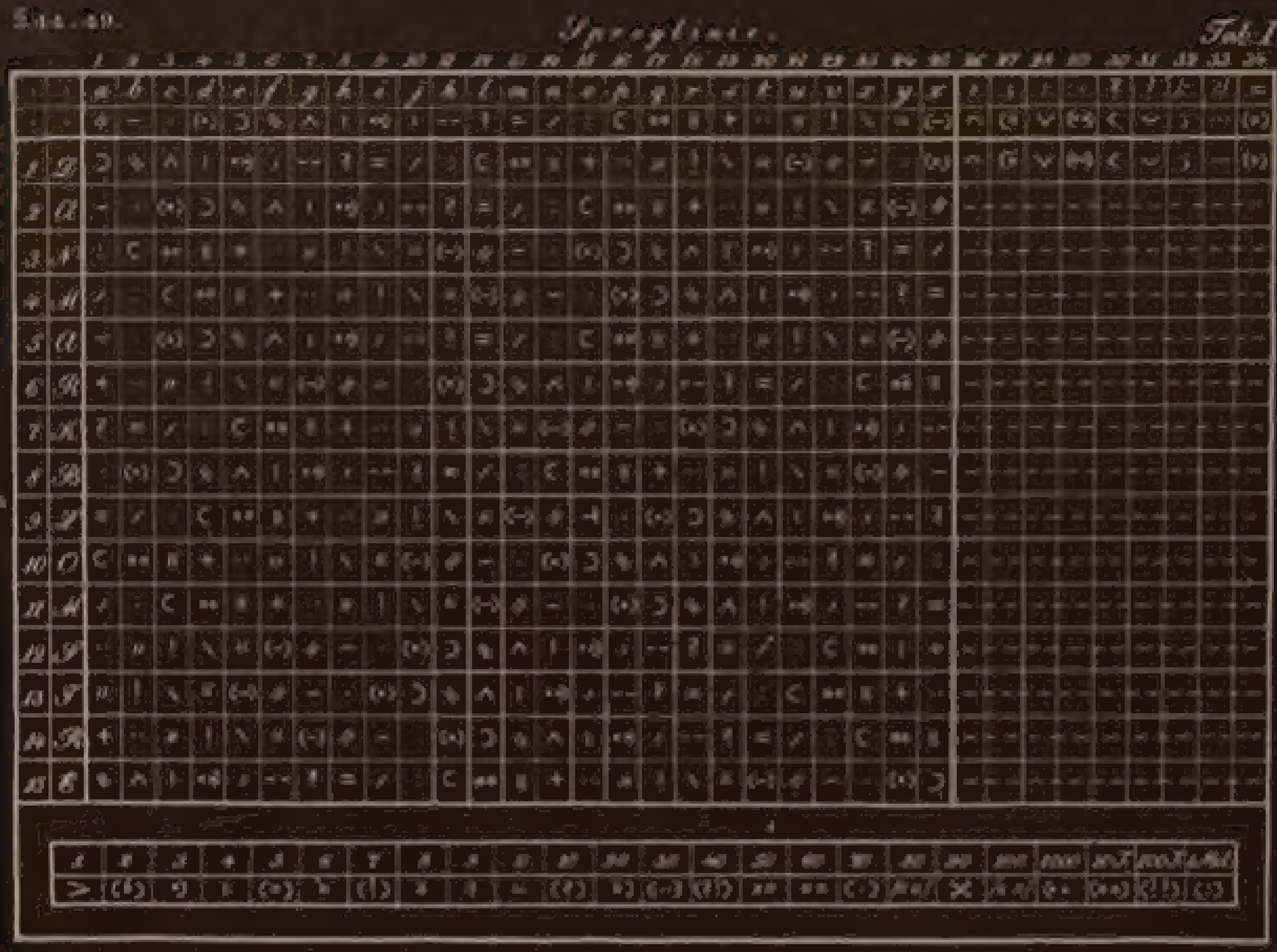
39) The letters which are now kept in the Greater London Record Office (Ref. A/RSA), are published by permission of the Royal Society of Arts. I am indebted to Mr. D.G.C. Allan, Curator-Librarian of the Royal Society of Arts, and Miss J. Coburn, Head Archivist of the Greater London Record Office, for their help in locating this material. Also, I wish to thank Dr. Janet Efstathiou, Queen Mary College, who has aided me in this search.

40) *Memoirs and Correspondence by Major-General H.P. Babbage*. Privately printed by the firm of William Clowes, London, 1915, pp. 81-82. I am indebted to Mr. Garry J. Tee for providing me with a transcript of this passage.

41) I am grateful to Mr. Garry J. Tee who, on his own accord, went to the British Library to check my transcript of the Williamson letter and to search the index of manuscripts for the names of Williamson and Hammond.
I also wish to thank Mr. R.A.H. Smith, Assistant Keeper, Dept. of Manuscripts, The British Library, for his kind and invaluable help, enabling me to bring the various illustrations from Babbage's cryptographical file in the British Library.

42) K. Iverson, *op.cit.* (note 45, part 1).

43) O.I. Franksen, *op.cit.* (note 13, part 2).



From the foreword by H. H. Goldstine

Although it may be read as an entertaining account of the cryptographical works of Babbage and others, the reader will find that the subject area of 19th century secret writing is not a goal in itself, but rather a vehicle. Neither is it a textbook presenting an educational introduction to APL. What fascinated Franksen and, I think, what will fascinate the reader, is Babbage's groping towards an understanding of the innermost nature of data and data operations. . . . It is in this light that he sees Babbage's attempts to cast cryptography into a formalized mathematical formulation.

It is his intriguing thought, given a popular exposition in this book, that the data concept of APL reduces to the definition of a geometry in the sense of Felix Klein's famous Erlanger Program of 1872. This opens an entirely new perspective in the educational integration of the computer into the traditional sciences and their areas of application.

PRENTICE-HALL, INC., Englewood Cliffs, N.J. 07632

ISBN 0-13-604729-7